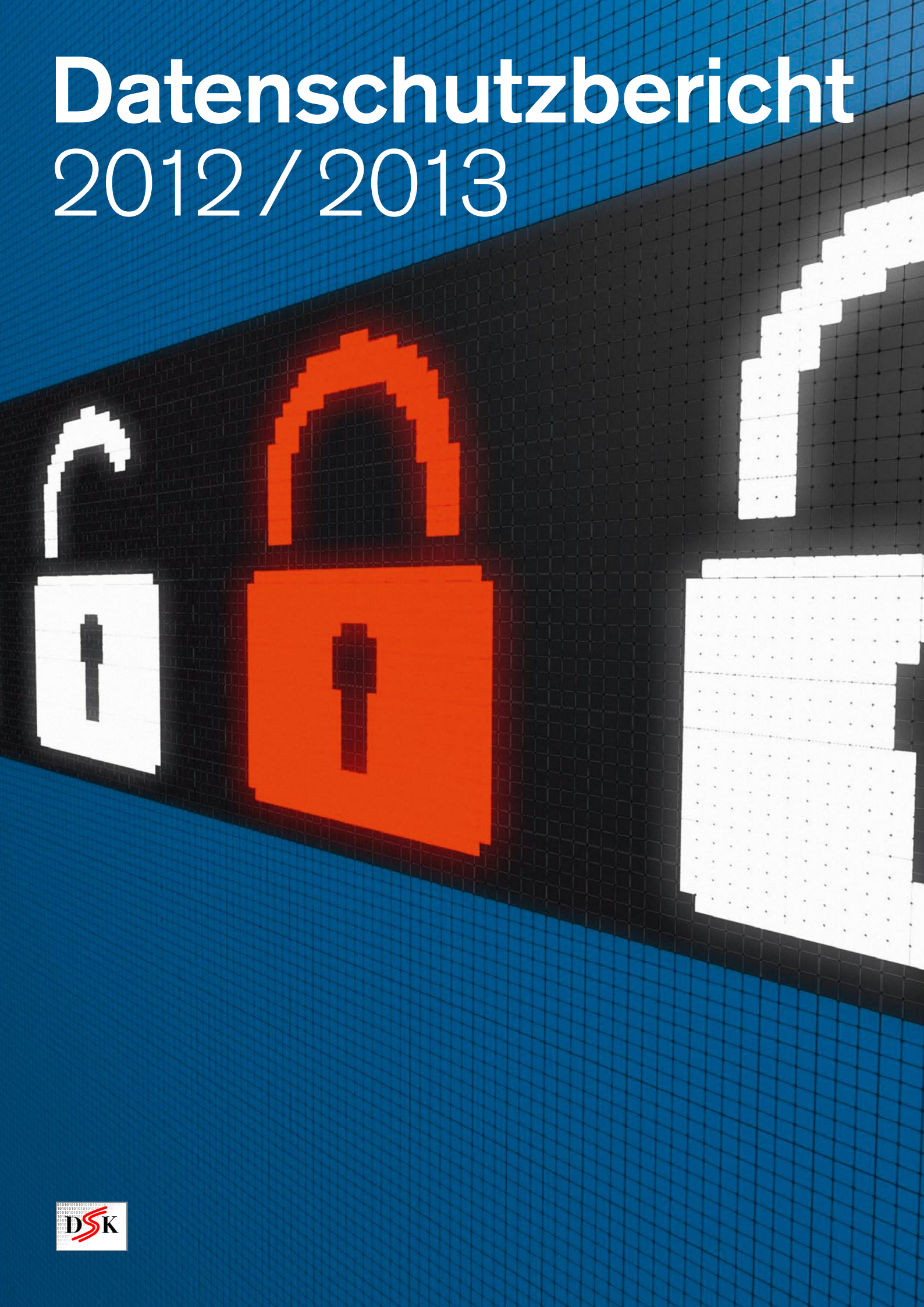
Datenschutzbericht 2012 / 2013



Datenschutzbericht 2012 – 2013

Wien, 2014

Impressum

Medieninhaber, Herausgeber und Redaktion:
Datenschutzkommission
(gemäß § 35ff DSG 2000), Hohenstaufengasse 3, 1010 Wien
Kontakt: dsb@dsb.gv.at
Website: www.dsb.gv.at

Fotonachweis: BKA | ARGE Grafik
Gestaltung: BKA | ARGE Grafik
Druck: BM.I Digitalprintcenter
Wien, 2014

Inhalt

1 Einleitung

Die Datenschutzkommission (DSK) ist bzw.. war bis Ende 2013 die nationale Datenschutz-Kontrollstelle im Sinne des Art.28 der Datenschutzrichtlinie 95/46/EG.

Ihr hiermit vorgelegter fünfzehnter Datenschutzbericht umfasst den Zeitraum vom 1. Jänner 2012 bis 31. Dezember 2013. Es handelt sich hierbei um den letzten Datenschutzbericht der Datenschutzkommission, da diese am 31. Dezember 2013 aufgelöst und durch eine neue Datenschutzbehörde ersetzt wird.

Der Datenschutzbericht enthält einige grundsätzliche Ausführungen zur Situation der Datenschutz-Kontrollbehörde in Österreich. In diesem Zusammenhang wird auch die Rechtslage infolge der im Berichtszeitraum beschlossenen Verwaltungsgerichtsbarkeits-Novelle 2012[1] (vgl. Pkt. 5.4. des 14. Datenschutzberichtes, der sich noch auf die Regierungsvorlage der Verwaltungsgerichtsbarkeits-Novelle 2012 bezog) und der im Kontext dazu ergangenen DSG-Novelle 2014 dargestellt.

In den Berichtszeitraum fallen auch die ersten Erfahrungen mit der am 1. Mai 2013 in Kraft getretenen DSG-Novelle 2013, mit der die Datenschutzkommission aus dem Bundeskanzleramt ausgegliedert und als eigene Dienstbehörde und Personalstelle eingerichtet wurde.

Zur besseren Erkennbarkeit von Entwicklungen nehmen die statistischen Schaubilder so wie im letzten Bericht auch auf vorhergehende Amtsperioden der Datenschutzkommission Bezug.

Soweit in diesem Bericht auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.

1 BGBl I Nr. 2/2012.

2 Die Organe der Datenschutzkommission

Als Organe der Datenschutzkommission werden das Kollegium der Mitglieder als Kollegialorgan, weiters in bestimmten Angelegenheiten der Vorsitzende und aufgrund des § 38 Abs. 1 DSG 2000 das in der Geschäftsordnung bestimmte geschäftsführende Mitglied (GfM) – jeweils allein – tätig.[2]

Die folgenden Ausführungen beziehen sich – sofern nicht ausdrücklich auf die Rechtslage ab 1. Jänner 2014 hingewiesen wird – auf die bis 31. Dezember 2013 geltende Rechtslage.

2.1 Zur rechtlichen Stellung der Mitglieder der Datenschutzkommission

»Die Mitglieder der Datenschutzkommission sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden« (§ 37 Abs. 1 DSG 2000). Diese Bestimmung, die 2008 im Zuge der Bereinigung von außerhalb des B-VG stehenden Verfassungsbestimmungen ihres Verfassungsrangs entkleidet wurde[3], ist vor dem Hintergrund des im Jahre 2008 novellierten Art. 20 Abs. 2 B-VG[4] zu sehen, der die Voraussetzungen für das Bestehen weisungsfreier Verwaltungsbehörden allgemein regelt. Nähere Ausführungen zu den Konsequenzen dieser Neuregelung finden sich in Kapitel 6.

Seit 1. Juli 2000 beträgt die Zahl der Kommissionsmitglieder und Ersatzmitglieder jeweils sechs Personen, die vom Bundespräsidenten ernannt werden. Durch die Datenschutzgesetz-Novelle 2010 wurde verbindlich festgeschrieben, dass sämtliche Mitglieder der Datenschutzkommission ihre Tätigkeit in der Datenschutzkommission nur neben ihrem Hauptberuf ausüben (vgl. § 36 Abs. 3a). Gleichzeitig wurde durch die DSG-Novelle 2010 klargestellt, dass als richterliches Mitglied sowie als geschäftsführendes Mitglied nur aktive Richter bzw. Bundesbedienstete tätig sein können und es wurde für die übrigen Mitglieder eine Altersgrenze von 65 Jahren eingeführt.[5]

Der für die Ernennung der Mitglieder der Datenschutzkommission durch den Bundespräsidenten notwendige Vorschlag der Bundesregierung wird erstattet hinsichtlich

- des richterlichen Mitglieds und des richterlichen Ersatzmitgliedes aufgrund eines Dreiervorschlages des Präsidenten des OGH,
- zweier Mitglieder und zweier Ersatzmitglieder aufgrund eines Vorschlags der Länder,
- eines Mitglieds und eines Ersatzmitglieds aufgrund eines Dreiervorschlags der Bundeskammer für Arbeiter und Angestellte, sowie hinsichtlich
- eines Mitglieds und eines Ersatzmitglieds aufgrund eines Dreiervorschlags der Wirtschaftskammer Österreich.

Ein Mitglied und ein Ersatzmitglied sind von der Bundesregierung aus dem Kreis der Bundesbediensteten[6] vorzuschlagen.

2 »Die Datenschutzkommission hat sich eine Geschäftsordnung zu geben, in der eines ihrer Mitglieder mit der Führung der laufenden Geschäfte zu betrauen ist« (§ 38 Abs. 1 DSG 2000, Verfassungsbestimmung).
3 BGBl I Nr. 2/2008.
4 BGBl I Nr. 2/2008.
5 Vgl. § 36 Abs. 6 DSG 2000 idF der DSG-Novelle 2010.
6 Vgl. Neufassung des § 36 Abs. 3 DSG 2000 durch die DSG-Novelle 2010.

2.2 Die Mitglieder der Datenschutzkommission im Berichtszeitraum

Die Zusammensetzung der Datenschutzkommission von 1. Jänner 2012 bis 31. Dezember 2013 war wie folgt:

Mitglieder:
- Dr. Anton Spenling, Vorsitzender (richterliches Mitglied)
- Dr. Eva Souhrada-Kirchmayer, geschäftsführendes Mitglied
- Mag. Helmut Hutterer
- Dr. Claudia Rosenmayr-Klemenz
- Dr. Klaus Heissenberger
- Mag. Daniela Zimmer

Ersatzmitglieder:
- Dr. Gerhard Kuras, stv. Vorsitzender (richterliches Ersatzmitglied)
- Dr. Gregor König, LLM, stv. geschäftsführendes Mitglied
- Dr. Michaela Blaha
- Mag. Huberta Maitz-Strassnig
- Dr. Josef Gundacker
- Mag. Gerda Heilegger

2.3 Die Organe der Datenschutzkommission

2.3.1 Das Kollegium der Datenschutzkommission

Die Datenschutzkommission als Kollegialorgan hat die rechtliche Stellung eines Tribunals iSd EMRK: Ihre Mitglieder sind in dieser Funktion weisungsfrei, ihr Vorsitzender ist Richter. Die Datenschutzkommission ist allerdings keine Art. 133 Z 4 B-VG Behörde, sondern auch organisatorisch eine Behörde sui generis (vgl. die §§ 36 ff DSG 2000). Art. 20 Abs. 2 B-VG (neu) bietet eine verfassungsrechtliche Grundlage für die Weisungsfreiheit solcher Verwaltungsbehörden.

Der Datenschutzkommission als Kollegialbehörde obliegt vor allem die Beschlussfassung hinsichtlich der rechtsförmlichen Entscheidungen der Datenschutzkommission im Verfahren nach § 31 DSG 2000 sowie die Beschlussfassung in allen Angelegenheiten von richtungsweisender Bedeutung (vgl. § 38 Abs. 1 DSG 2000 und die in Ausführung hiezu ergangene Geschäftsordnung der Datenschutzkommission).

2.3.2 Der Vorsitzende

Der Vorsitzende vertritt die Datenschutzkommission nach außen, soweit er dies nicht im Einzelfall an andere Mitglieder übertragen hat (vgl. hiezu § 2 Abs. 1 der Geschäftsordnung).

Der Vorsitzende führt weiters den Vorsitz in den Sitzungen des Kollegiums der Datenschutzkommission; die Beschlüsse des Kollegiums werden von ihm gefertigt.

Seit 1. Mai 2013[7] übt der Vorsitzende die Diensthoheit über die Bediensteten der Geschäftsstelle aus. Er hat aber den Großteil dieser Agenden aufgrund § 7 Abs. 3 der Geschäftsordnung

7 Inkrafttreten der DSG-Novelle 2013, BGBl. I Nr. 57/2013

der Datenschutzkommission[8] an das Geschäftsführende Mitglied der Datenschutzkommission delegiert. Ebenso hat er die Weisungsbefugnisse bezüglich der laufenden Geschäfte an das Geschäftsführende Mitglied delegiert.

2.3.3 Das Geschäftsführende Mitglied

Das Geschäftsführende Mitglied (in der Folge: GfM) führt die täglichen Geschäfte der Datenschutzkommission. Hiezu gehören nach der Geschäftsordnung der Datenschutzkommission auch die meisten Angelegenheiten, die keiner Beschlussfassung durch das Kollegium bedürfen, wie insbesondere die Erledigung von Ombudsmann-Verfahren (nicht aber z. B. die Erstattung von Empfehlungen) oder die Vornahme von Registrierungen im Datenverarbeitungsregister (nicht aber z. B. die Ablehnung einer Registrierung).

In wichtigen Fragen stellt das GfM das Einvernehmen mit dem Vorsitzenden her. Es hat weiters das Recht, das Kollegium jederzeit mit einer Angelegenheit zu befassen, ohne dass dies allerdings einen Kompetenzübergang zur Entscheidung zur Folge hätte.

Seit 1. Mai 2013 übt das GfM aufgrund der Delegation dieser Agenden durch den Vorsitzenden an das GfM die Dienstaufsicht über die Bediensteten der Geschäftsstelle aus. Von dieser Delegation ausgenommen ist die Dienstaufsicht des Vorsitzenden über das GfM selbst.

2.4 Die Datenschutzkommission als Stammzahlenregisterbehörde

Aufgrund § 9 des E-Government-Gesetzes hat die Datenschutzkommission auch die Rolle der Stammzahlenregisterbehörde wahrzunehmen. Mit dieser Funktion ist vor allem die Verantwortung für die sichere und ordnungsgemäße Erzeugung und Verwendung der Stammzahlen verbunden sowie die Erlaubnis, bereichsspezifische Personenkennzeichen zu verwenden (vergleiche hierzu Näheres im Kapitel 9).

Die Vollziehung des E-Government-Gesetzes fällt, sofern nicht ausnahmsweise mit Bescheid vorzugehen wäre, in die Zuständigkeit des GfM.

8 Geschäftsordnung der Datenschutzkommission vom 30. April 2013.

3 Die Geschäftsstelle der Datenschutzkommission

3.1 Aufgaben und Organisation der Geschäftsstelle

Die Geschäftsstelle unterstützt die Datenschutzkommission in allen Angelegenheiten der Datenschutzkommission, einschließlich ihrer Aufgaben als Stammzahlenregisterbehörde. In der Geschäftsstelle sind zwei Referate eingerichtet, nämlich das Büro der Datenschutzkommission, das für die vorbereitende Behandlung der Beschwerdefälle zuständig ist, und das Datenverarbeitungsregister (DVR).

Gemäß § 37 Abs. 2 DSG 2000 ist im Bundesfinanzgesetz die notwendige Sach- und Personalausstattung sicherzustellen. Dies gilt auch für das DVR, dessen technische Aufrüstung Voraussetzung für das Inkrafttreten der neuen Bestimmungen in der DSG-Novelle 2010 über die Online-Registrierung war.

Bis Ende April 2013 führte der Bundeskanzler die Dienstaufsicht über die Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle der Datenschutzkommission. Bis dahin war die der Datenschutzkommission zur Unterstützung in der Geschäftsführung beigegebene Geschäftsstelle organisatorisch als Abteilung im Verfassungsdienst des Bundeskanzleramtes eingerichtet. Seit 1. Mai 2013 ist die Datenschutzkommission eine eigene Dienstbehörde und Personalstelle.

3.2 Der Personalstand der Geschäftsstelle

Am Ende des Berichtszeitraumes verfügte die Geschäftsstelle über insgesamt 21,85 Planstellen auf Vollbeschäftigungsäquivalent-Basis mit folgender Wertigkeit;

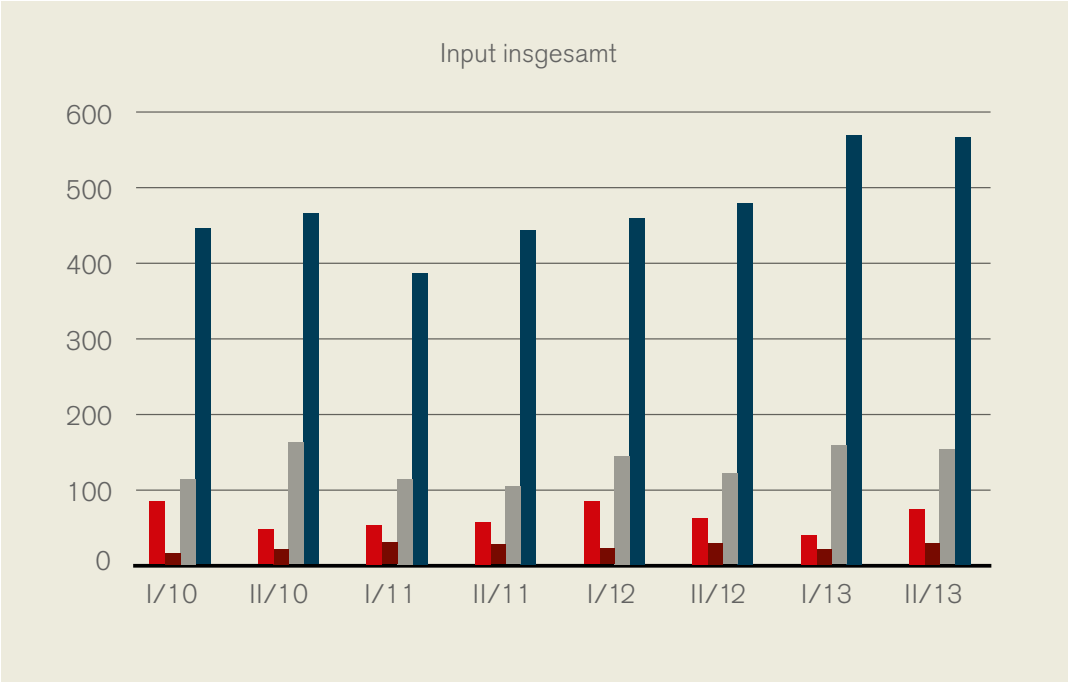
- 12 A/a Planstellen (einschließlich einer Behinderten-Planstelle),
- 3 B/b Planstellen und
- 6,65 C/c Planstellen

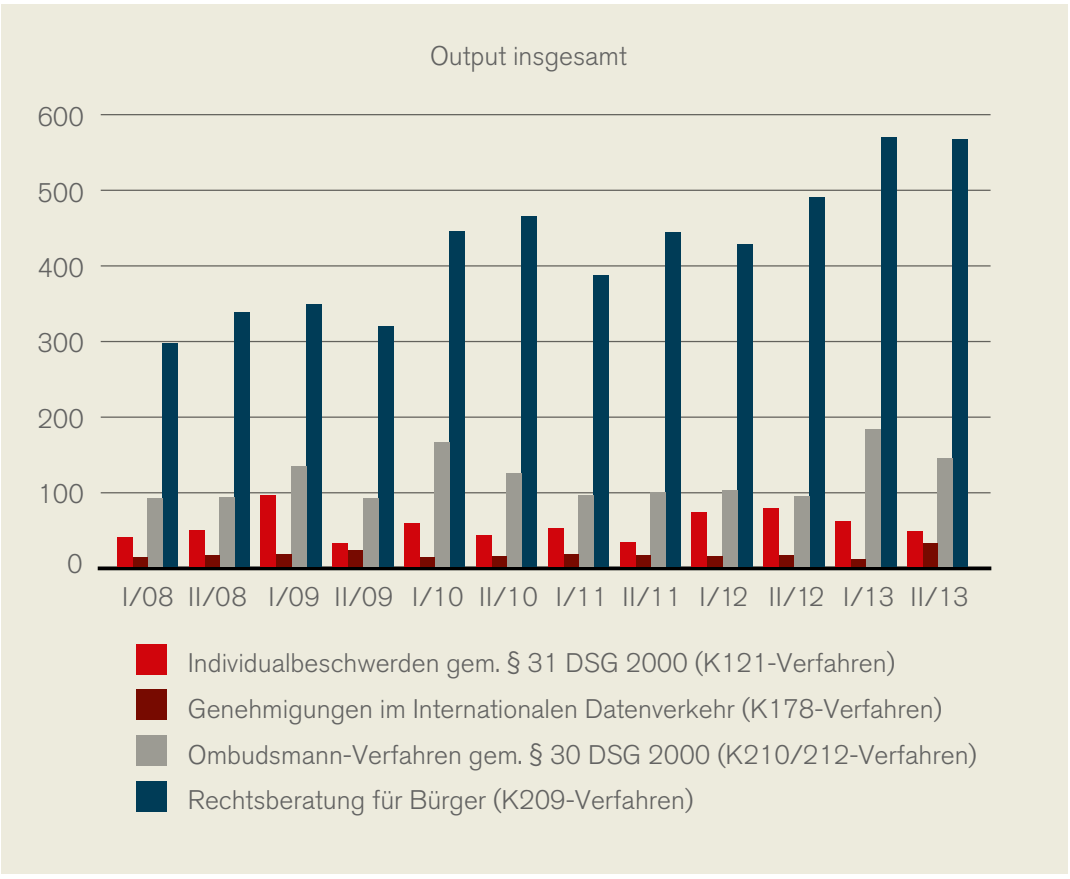
Davon entfielen 12,35 Planstellen auf das Datenverarbeitungsregister und 9,5 Planstellen auf den restlichen Teil der Geschäftsstelle.

Wie bereits berichtet, war im Rahmen des Budgetbegleitgesetzes (BGBl. I Nr. 112/2011) eine DSG-Novelle beschlossen worden, mit der der Zeitpunkt, zu dem die neue DVR-Verordnung spätestens erlassen werden muss, vom 1. Jänner 2012 auf den 1. September 2012 verschoben wurde. Hintergrund für diese Novelle war die Tatsache, dass das Unternehmensserviceportal, über das auch ein Großteil der DVR-Meldungen läuft, erst später als geplant zur Verfügung stand. Mit 1. September 2012 trat der Teil der DSG-Novelle 2010, mit dem ein Umstieg auf DVR-Online vorgesehen war, letztendlich in Kraft. Seither darf eine Meldung an das DVR grundsätzlich nur mittels automationsunterstützten Internet-Tools erfolgen.

4 Geschäftsgang

4.1 Statistische Darstellung des Geschäftsganges (Gesamtübersicht)



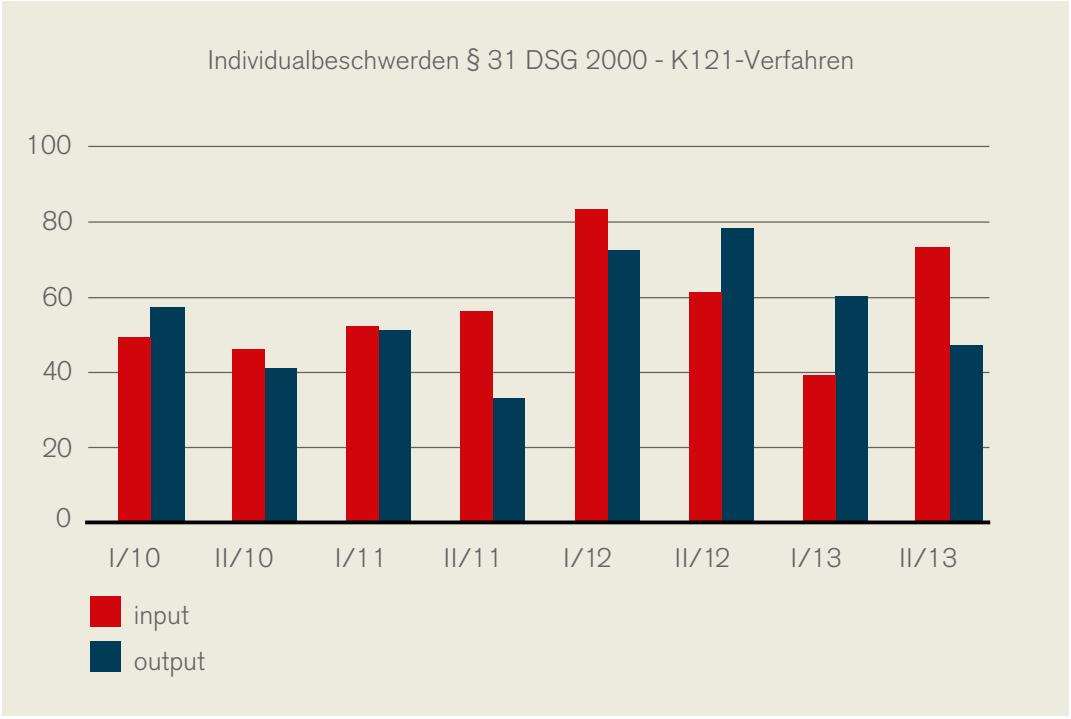


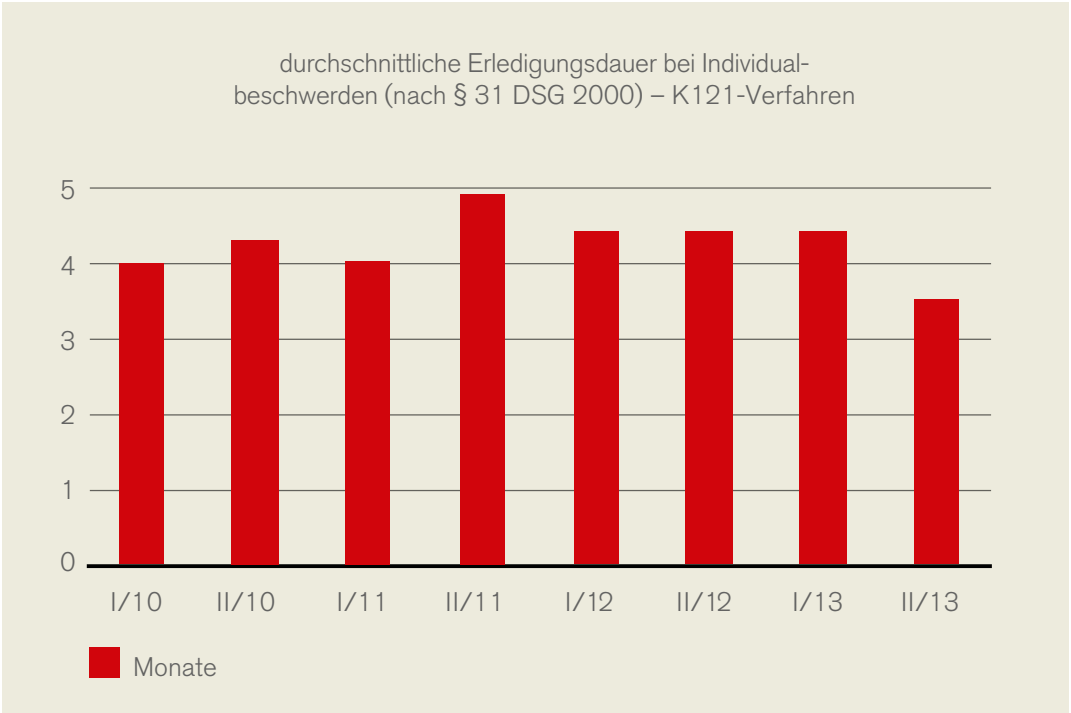
	Eingangsstücke				Erledigungen			
	1. Halb-jahr 2012	2. Halb-jahr 2012	1. Halb-jahr 2013	2. Halb-jahr 2013	1. Halb-jahr 2012	2. Halb-jahr 2012	1. Halb-jahr 2013	2. Halb-jahr 2013
Individualbeschwerden (K121-Verfahren)	83	61	151	73	72	78	60	47
Ombudsmannverfahren nach § 30 DSG 2000 (K210+K212)	143	129	157	152	101	93	182	144
Rechtsauskünfte (K209)	458	478	568	565	427	489	568	565
Genehmigungen nach § 46 und 47 DSG 2000 (K202)	2	9	5	5	3	6	7	1
Genehmigungen im Internationalen Datenverkehr (K178)	21	28	20	28	14	15	10	31
Auskunft Schengen (K250)	20	16	21	21	20	16	18	21
Erledigungen	1. Halbjahr 2012		2. Halbjahr 2012		1. Halbjahr 2013		2. Halbjahr 2013	
Entscheidungen der Kommission im Registrierungsverfahren (K503 und K600)	18		3		3		2	

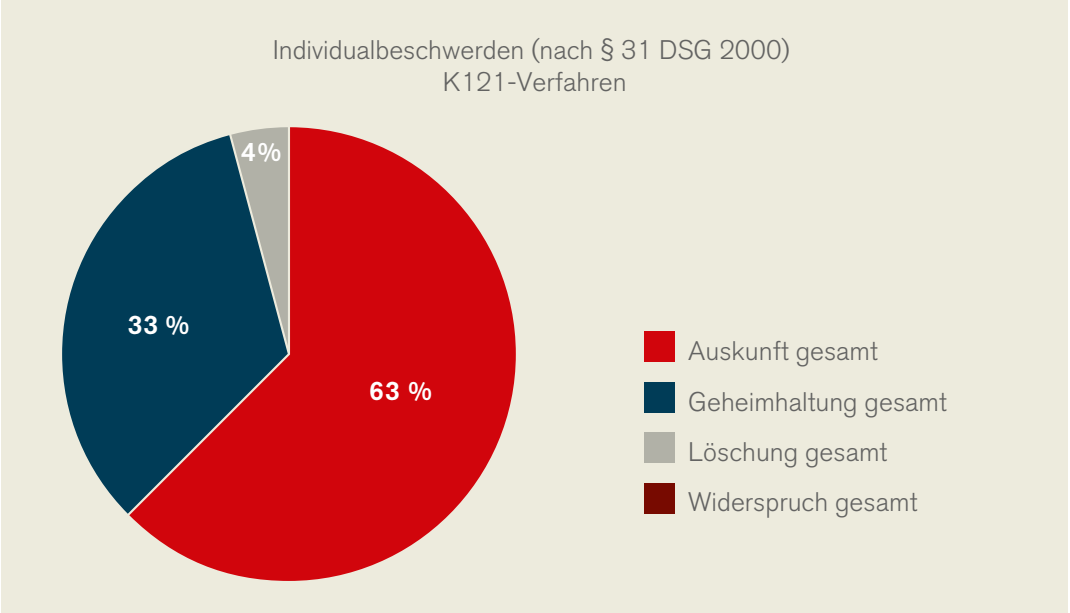
4.2 Die Verfahren vor der DSK

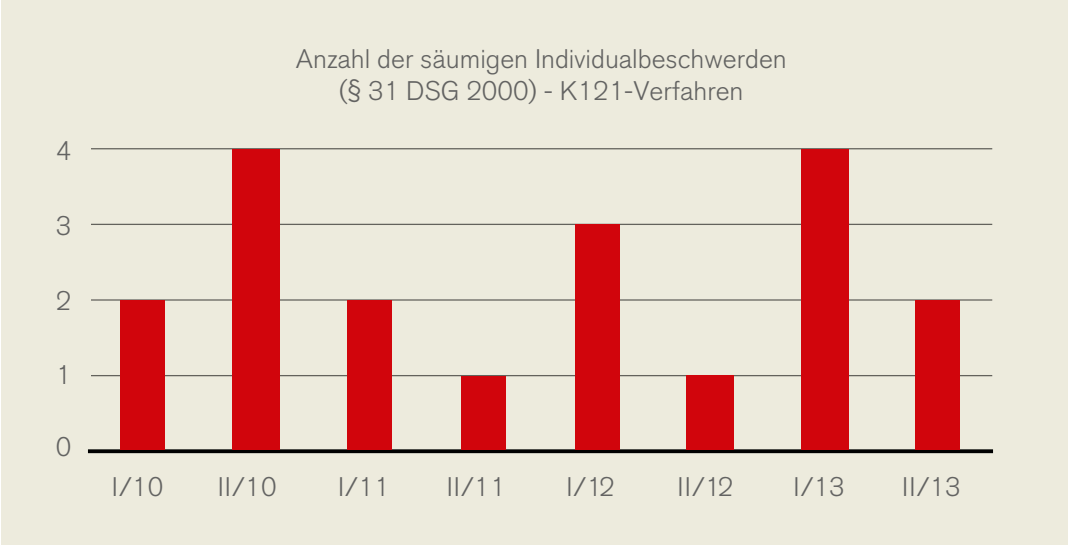
4.2.1 Individualbeschwerdeverfahren (§ 31 DSG 2000)

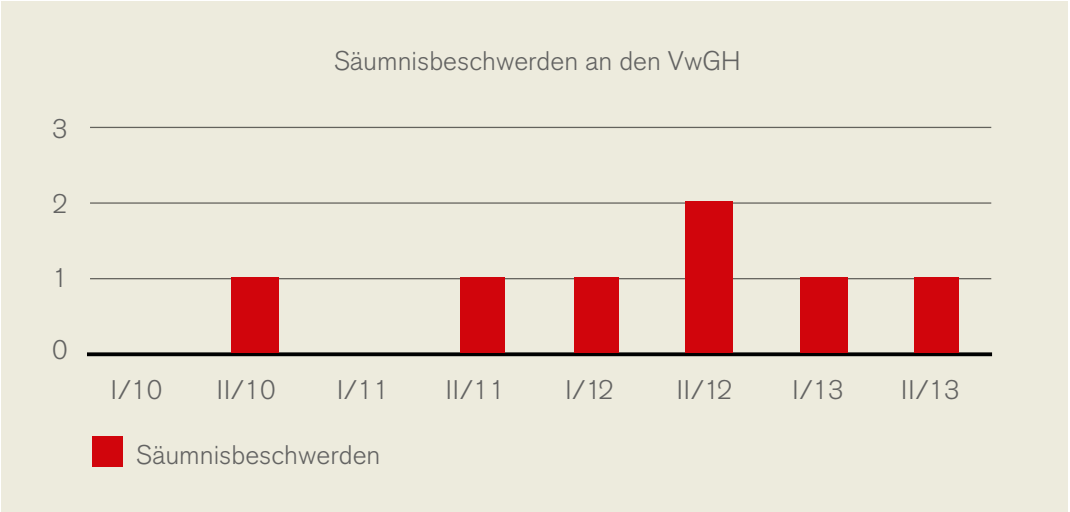
Gemäß § 31 DSG 2000 kann vor der DSK Beschwerde mit verbindlicher Wirkung der Entscheidung in Auskunftssachen (im privaten und öffentlichen Bereich) sowie in Geheimhaltungs-, Richtigstellungs- und Löschungssachen (nur hinsichtlich des öffentlichen Bereichs) erhoben werden.



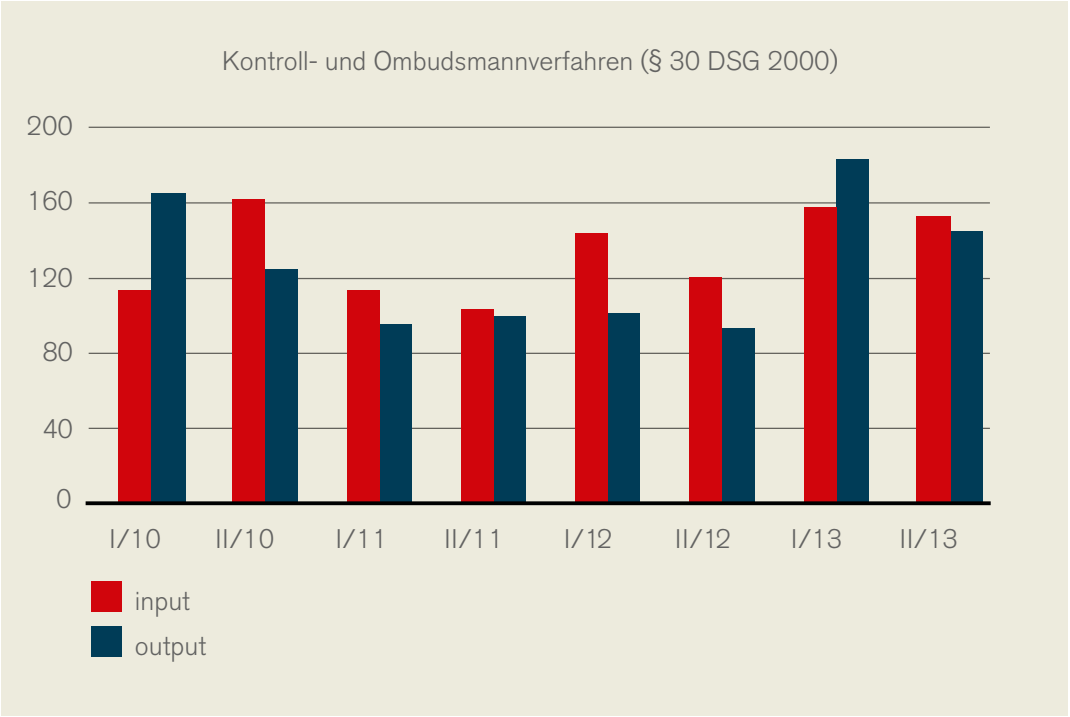



Individualbeschwerden (nach § 31 DSG 2000)
K121-Verfahren
4%
33 %
63 %
Auskunft gesamt
Geheimhaltung gesamt
Löschung gesamt
Widerspruch gesamt


Anzahl der säumigen Individualbeschwerden
(§ 31 DSG 2000) - K121-Verfahren
4
3
2
1
0
I/10
II/10
I/11
II/11
I/12
II/12
I/13
II/13


Säumnisbeschwerden an den VwGH
3
2
1
0
I/10
II/10
I/11
II/11
I/12
II/12
I/13
II/13
Säumnisbeschwerden

4.2.2 Ombudsmannverfahren



Hier war im Berichtszeitraum gegenüber den Vorjahren ein Ansteigen des Arbeitsanfalls zu beobachten.

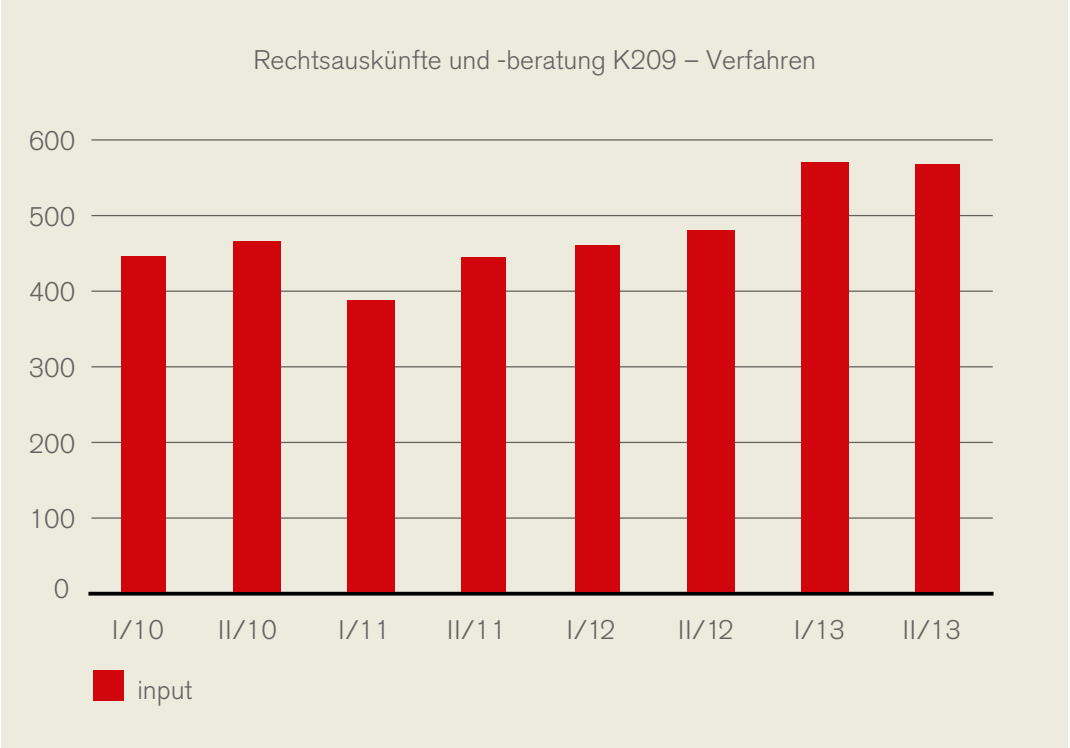
Das Ombudsmannverfahren hat sich als äußerst wertvolles Instrument der Rechtsverwirklichung erwiesen. Die weitgehende Formfreiheit dieses Verfahrens ermöglicht – meistens – eine besonders rasche Erledigung der Anliegen der Bürger. Obwohl hier keine unmittelbar durchsetzbaren Entscheidungen erlassen werden, führt die Tätigkeit der DSK dennoch in fast allen Fällen zu einem für die Beschwerdeführer zufrieden stellenden Ergebnis.

Etwa 90 % der Eingaben im Ombudsmannverfahren betreffen den privaten Bereich, etwa 15 % sind daneben amtswegig durchgeführte Verfahren (siehe auch 4.2.6.), entweder aufgrund einer Eingabe einer nicht betroffenen Person oder aufgrund eigener Wahrnehmung der DSK.

4.2.3 Rechtsauskünfte an Bürger (K-209-Verfahren)

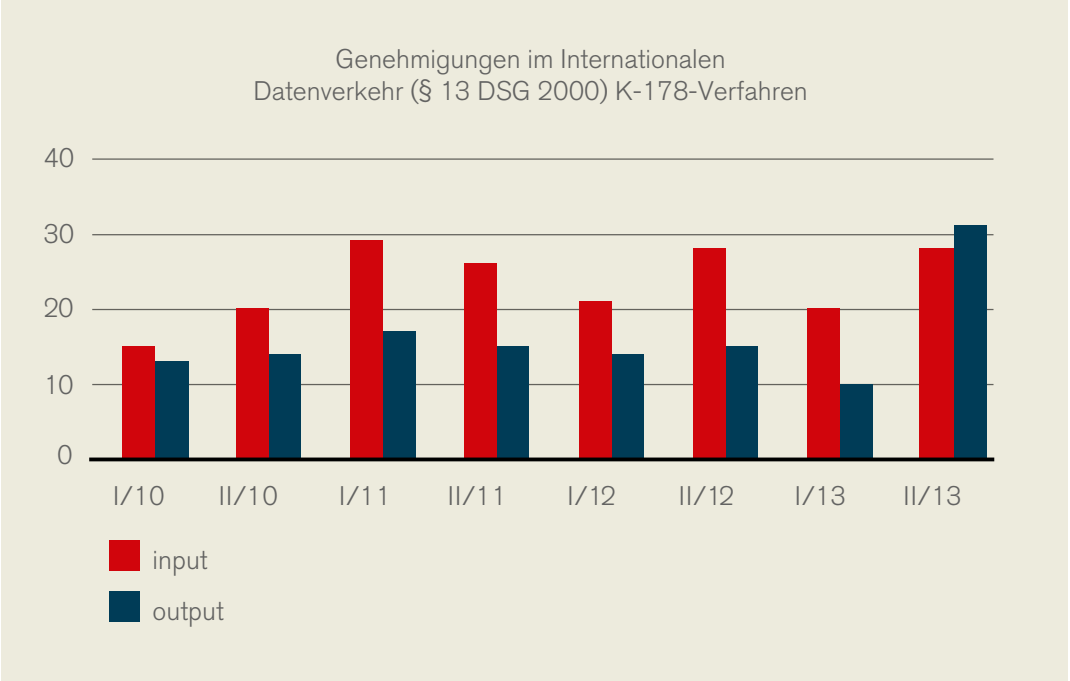
Wie wichtig diese vom Büro der DSK wahrgenommene Funktion geworden ist, ergibt sich anschaulich aus der untenstehenden Graphik. In dieser Statistik sind die zahlreichen telefonischen Auskünfte nicht enthalten, über deren Häufigkeit keine Aufzeichnungen geführt werden.

Hinzu kommt noch die Tätigkeit des DVR auf diesem Gebiet, das von der Bevölkerung nicht immer nur mit Rechtsfragen des Registrierungsverfahrens befasst wird. 90 Anrufe am Tag sind im DVR keine Seltenheit.



4.2.4 Genehmigungen im Internationalen Datenverkehr (§§ 12 und 13 DSG 2000):

Graphische Darstellung von Input und Output im Bereich »Internationaler Datenverkehr«:



Die bereits im vorigen Berichtszeitraum erreichte Beschleunigung der Verfahren durch Beseitigung von Unklarheiten in diesem Bereich zeigte sich teilweise auch in den Jahren 2010 und 2011.

Dass Genehmigungsverfahren nach wie vor gelegentlich mehr als sechs Monate in Anspruch nehmen, ist darauf zurückzuführen, dass das Genehmigungsverfahren eine registrierungsfähige Meldung jener Datenanwendung voraussetzt, aus der die Daten übermittelt bzw. überlassen werden sollen.

4.2.5 Bescheide der DSK im Registrierungsverfahren (§ 20 Abs. 4 und § 21 Abs. 2 DSG 2000)

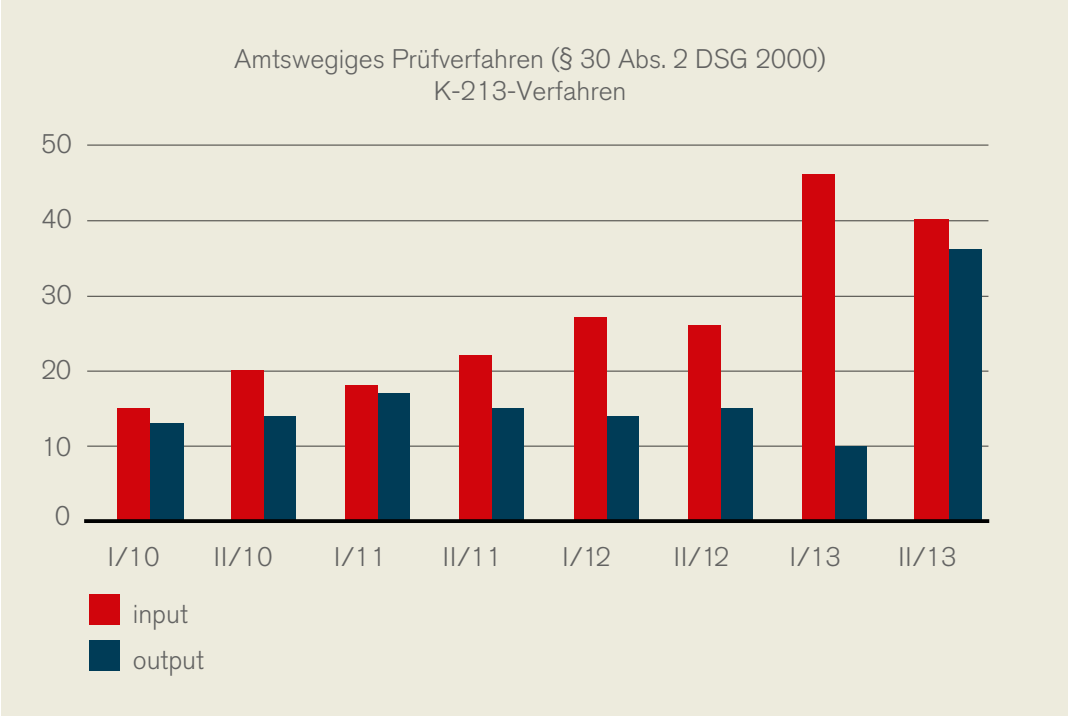
Die Registrierung der Meldung einer Datenanwendung erfolgt nicht mit Bescheid, sondern mit bloßer Mitteilung, die nicht der Rechtskraft fähig ist (der meldende Auftraggeber erwirbt durch die Registrierung keinen Rechtsanspruch darauf, die Datenanwendung in der gemeldeten Form durchführen zu dürfen). Ein Bescheid der DSK ergeht nur dann, wenn die Registrierung einer Meldung (ganz oder teilweise) abgelehnt wird oder wenn bei vorabkontrollpflichtigen Datenanwendungen (§ 18 Abs. 2 DSG 2000) Auflagen für die Führung der Datenanwendung im Interesse des Schutzes der Betroffenenrechte notwendig sind.

Im Berichtszeitraum hat sich die Notwendigkeit, Bescheide im Registrierungsverfahren zu erlassen, zum einen im Zusammenhang mit der Meldung von Videoüberwachungen ergeben, zum anderen bei der Einrichtung von Informationsverbundsystemen in einzelnen Branchen (vgl. hiezu auch die Ausführungen in Abschnitt 8) sowie Whistleblower-Systemen von Konzernen.

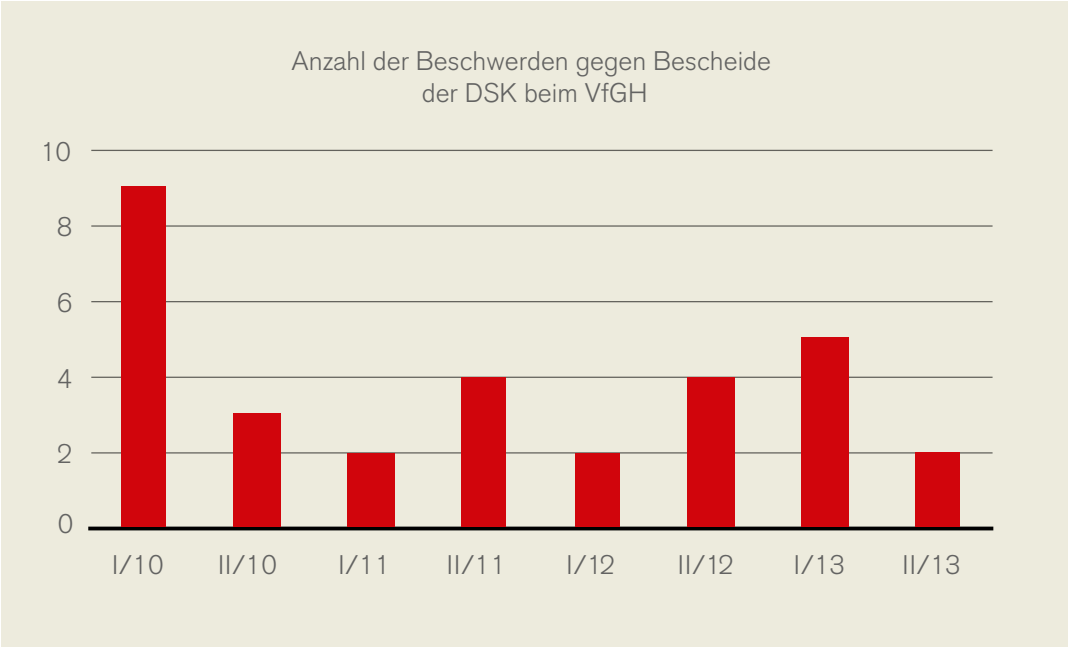
4.2.6 Amtswegige Prüfverfahren

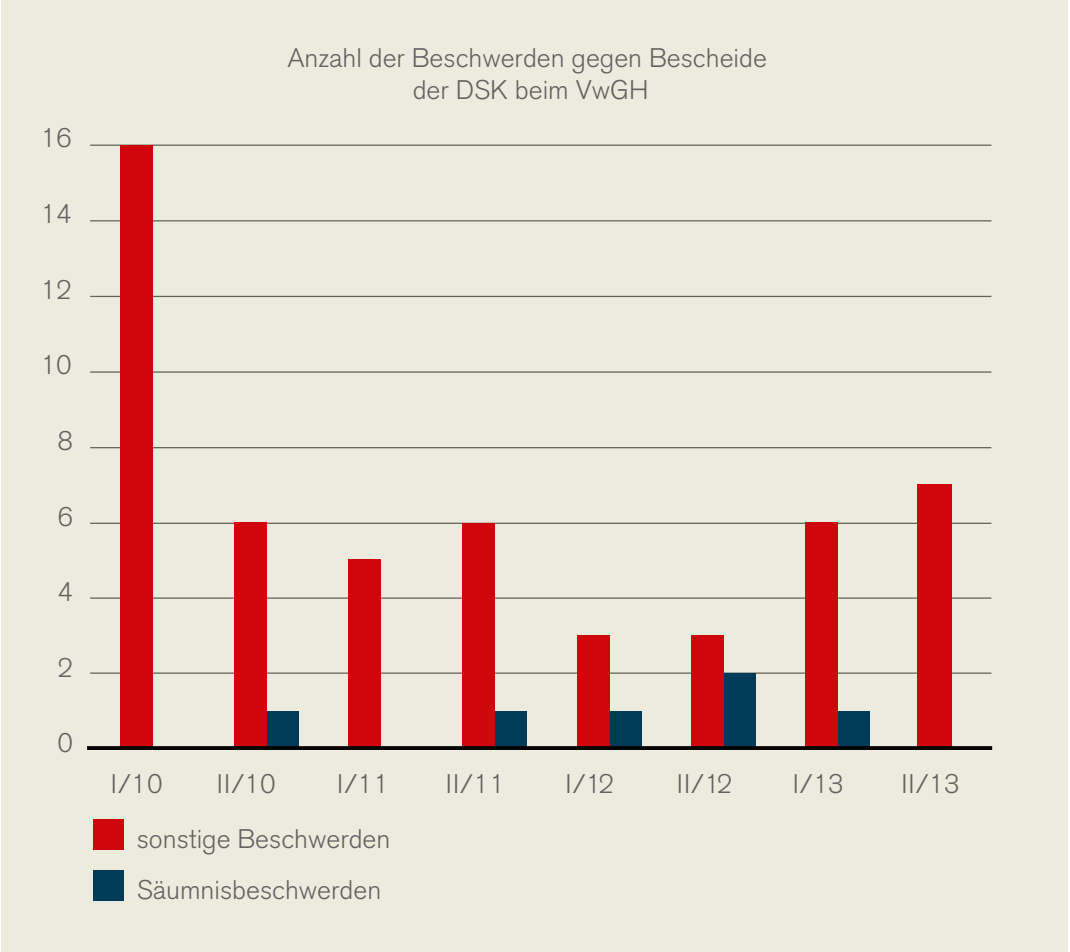
Diese haben sich im Berichtszeitraum hauptsächlich auf den Sektor Kreditinformation und Kreditauskunfteien konzentriert. Überdies wurden einige amtswegige Prüfverfahren im Zusammenhang mit den Hacking-Attacken von Anonymous Österreich eingeleitet, da in einigen Fällen der Verdacht der Verletzung von Datensicherheitsmaßnahmen gegeben war.

Dass die Tätigkeit der DSK auf diesem Sektor nicht die wünschenswerte Dichte erreicht, ist der DSK bewusst und wird außerordentlich bedauert, doch ist nicht absehbar, dass sich dieser Zustand bei der gegebenen Personalsituation verbessern ließe.



4.2.7 Äußerungen in Beschwerdeverfahren vor dem Verfassungs- und Verwaltungsgerichtshof





Von den 13 im Berichtszeitraum (2012 und 2013) gegen Bescheide der DSK erhobenen VfGH-Beschwerden sind zwei Fälle noch nicht entschieden, in 4 Fällen erfolgte eine Ablehnung, in 3 Fällen erfolgte eine Aufhebung, in 4 Fällen eine Abweisung, 2 Fälle sind noch nicht entschieden.

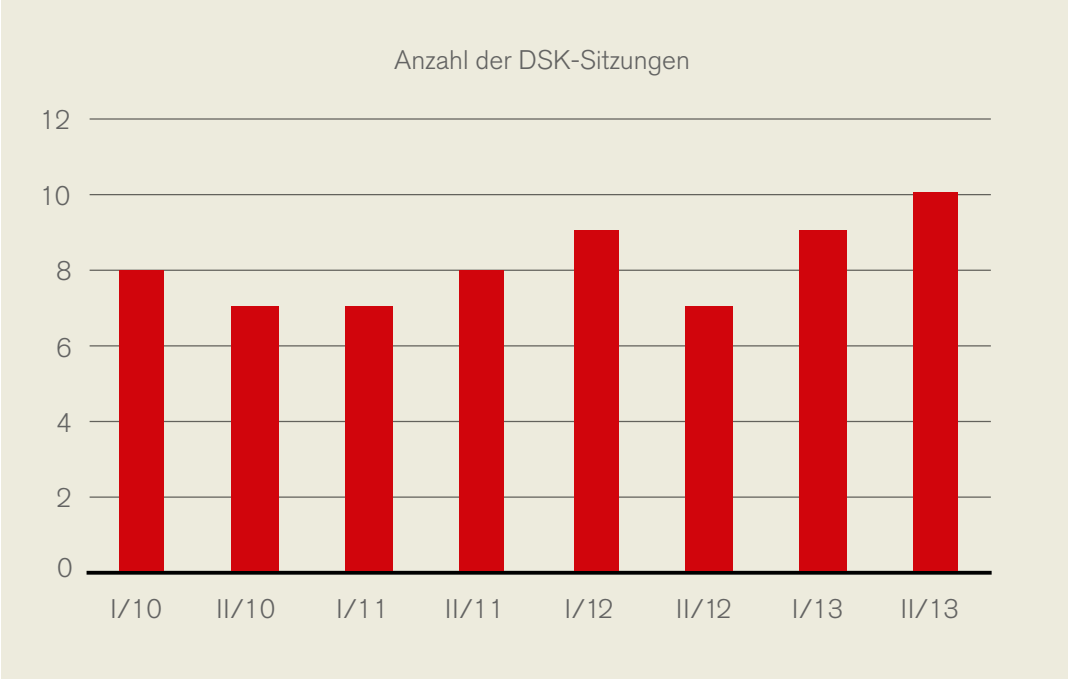
Im Berichtszeitraum 2012 wurde gegen 6 Bescheide der DSK Verwaltungsgerichtshofsbeschwerde erhoben, davon erfolgte in drei Fällen eine Abweisung; in den restlichen 3 Fällen steht die Entscheidung noch aus.

Im Berichtszeitraum 2013 wurde gegen 13 Bescheide der DSK Verwaltungsgerichtshofbeschwerde erhoben, davon erfolgte in 3 Fällen eine Abweisung, eine Einstellung, in zwei Fällen eine Bescheidaufhebung und 7 Fällen steht die Entscheidung noch aus.

Zu betonen ist, dass ein Großteil der Aufhebungen, beginnend mit dem Erkenntnis vom 24. April 2013, Zl. 2011/17/0156, wegen »Unzuständigkeit der belangten Behörde« erfolgte. Der Verwaltungsgerichtshof beruft sich dabei auf das Urteil des Gerichtshofs der Europäischen Union vom 16. Oktober 2012, Rs C-614/10, in welchem festgetellt wurde, dass die Datenschutzkommission nicht die Anforderungen der von Art. 28 der Datenschutzrichtlinien geforderten »völliger Unabhängigkeit« erfülle. Interssanterweise sah der Verfassungsgerichtshof die Datenschutzkommission trotz des Urteils als zur Bescheiderlassung zuständige Behörde an (Erkenntnis vom 14. März 2013, GZ B1326/12).

4.3 Sitzungen der Datenschutzkommission

Die DSK ist nur bei Anwesenheit aller sechs Mitglieder, allenfalls vertreten durch das zugehörige Ersatzmitglied, beschlussfähig. Eine Ausnahme hievon durch Beschlussfassung im Umlaufweg ist bei Beschwerdeverfahren nach § 31 DSG 2000 nur dann möglich, wenn im Umlaufverfahren nur mehr die Ausformulierung der Bescheidbegründung behandelt wird.



5 Kritische Anmerkungen zur Personalsituation der Datenschutzkommission

5.1 Zu den Aufgaben der Datenschutzkommission und ihrer Personalausstattung

5.1.1 Grundsätzliches zur Personalausstattung

Trotz punktueller Hilfestellung durch den Verfassungsdienst des Bundeskanzleramtes hat sich an der Tatsache, dass die Datenschutzkommission – gemessen an der Einwohnerzahl – viel weniger Personal besitzt als die meisten anderen Datenschutz-Kontrollstellen der Mitgliedsstaaten der Europäischen Union, grundsätzlich nichts geändert.[9] Einige dieser anderen Behörden wurden wiederholt aufgestockt, so dass die österreichische Behörde im Vergleich dazu entsprechend abfällt.

Das Datenverarbeitungsregister nimmt über 50 % der gesamten Personalressourcen der Geschäftsstelle in Anspruch, was angesichts des von der Geschäftsstelle zu besorgenden Aufgabenbündels nicht angemessen ist. Zwar fand durch das Inkrafttreten des letzten Teils der DSG-Novelle 2010 und die Einführung von DVR-Online (siehe weiter unten) eine Entlastung des Datenverarbeitungsregisters (DVR) statt, durch die technischen Anfangsschwierigkeiten (vor allem im Bereich des Unternehmensserviceportals) wurde das DVR allerdings monatelang durch eine Vielzahl von Anrufen belastet, sodass grundsätzliche Erleichterungen im Berichtszeitraum erst teilweise zum Tragen gekommen sind. Auch ist darauf hinzuweisen, dass die komplexen Fälle, die der Vorabkontrolle durch das DVR bedürfen, ca 50 % der Arbeit des DVR ausmachen und die abzuarbeitenden Altlasten des DVR erheblich sind.

Bisher war es daher nicht möglich, Personalumschichtungen vorzunehmen, zumal auch nach wie vor ein erheblicher Rückstau an Erledigungen im DVR besteht. Aus Sicht der Datenschutzkommission wäre es daher notwendig, eine Lösung für die erheblichen Altlasten des DVR vorzusehen und darüber hinaus die Vorabkontrollpflicht von Datenanwendungen zu reduzieren. Aus Sicht der Datenschutzkommission wäre es notwendig, im DVR im Hinblick auf die komplexen Vorabkontrollverfahren mehr höher qualifiziertes Personal (A- und B-Bedienstete) zum Einsatz zu bringen.

Eine weiter gehende Entlastung des DVR ist daher unabdingbar (siehe unten Kapitel 9 zum »gesetzlichen Handlungsbedarf«).

Im Bereich des Büros der Datenschutzkommission traten im Berichtszeitraum durch steigende Beschwerdezahlen und Ersuchen um Rechtsauskünfte regelmäßig Engpässe auf (siehe unten Punkt 5.1.3).

Im Übrigen wird nochmals darauf hingewiesen, dass von dem 1999 im Vorblatt zur Regierungsvorlage zum DSG 2000 unter »Kosten« ausgewiesenen zusätzlichen Bedarf von 4 Planstellen tatsächlich nur 2 (ab Ende 2012 nunmehr 3) Planstellen zugeteilt wurden, wobei seit Inkrafttreten des DSG 2000 vor allem im Bereich der Kontroll- und Ombudsmannverfahren nach § 30 DSG 2000 die Beschwerden signifikant gestiegen sind. Von dem im Vorblatt zur Regierungsvorlage zum E-GovG für das Stammzahlenregister veranschlagten Personalbedarf von 2 Planstellen steht nur eine zur Verfügung, die allerdings inzwischen auch für den internationalen Bereich herangezogen werden muss. Für einige neue Aufgaben der Datenschutzkommission (siehe unten Punkt 5.1.2) wurde überhaupt kein zusätzliches Personal zur Verfügung

9 Der Datenschutzkommission wurde im letzten Berichtszeitraum vom Verfassungsdienst des Bundeskanzleramtes eine zusätzliche juristische Planstelle zugeteilt. Damit kann ein Teil der stetig im Steigen befindlichen Kontrollverfahren abgedeckt werden.

gestellt. An dem Umstand, dass die österreichische Datenschutzkommission im europäischen Vergleich hinsichtlich ihrer Personalausstattung extrem unterdotiert ist, hat sich im Berichtszeitraum somit insgesamt nichts geändert.

5.1.2 Kontinuierliche Aufgabenerweiterung

Die Datenschutzkommission weist weiters darauf hin, dass durch die Erlassung neuer Gesetze, die intensiv in das Grundrecht auf Datenschutz eingreifen, höhere Beschwerde- und Fallzahlen zu erwarten sind bzw. diese bereits gegeben sind. Dies gilt für jene Gesetze, die im Zusammenhang mit der Umsetzung der Vorratsdatenspeicherung beschlossen wurden (TKG-Novelle sowie die die Abfrage regelnde StPO- und SPG-Novelle), aber auch für das Transparenzdatenbankgesetz und die SPG-Novelle 2011, mit der unter anderem die erweiterte Gefahrenerforschung auf Einzelpersonen ausgedehnt wurde. Weiters wurden durch die Umsetzung des so genannten »EU-Telekom-Pakets« in Form der »TKG-Novelle 2011« der Datenschutzkommission neue Befugnisse und Verpflichtungen (Entgegennahme der Meldung von Datenschutzverstößen, so genannte »Data Breach Notifications« und Erteilung von Anordnungen in diesem Zusammenhang, Kooperation mit der Regulierungsbehörde) eingeräumt bzw. auferlegt.

Auch im Zusammenhang mit dem im Berichtszeitraum beschlossenen »ELGA«-Gesetz (betreffend die Einrichtung einer »Elektronischen Gesundheitsakte«) wird mit weiteren Beschwerden an die Datenschutzkommission (zumindest im Rahmen von Kontroll- und Ombudsmannverfahren) zu rechnen sein.

Zu einem exorbitant hohen Arbeitsanfall bei der Stammzahlenregisterbehörde hat die Einrichtung der aufgrund des Transparenzdatenbankgesetzes eingerichteten »Transparenzdatenbank« geführt: Aufgrund des zitierten Gesetzes sind tausende Organisationen und Personen in das Ergänzungsregister einzutragen bzw. auch entsprechende Erstausstattungen von Organisationen mit bereichsspezifischen Personenkennzeichen (bPk) vorzunehmen. Der Gesetzgeber hat hiefür keinerlei zusätzliche Ressourcen für die Datenschutzkommission vorgesehen. Die Stammzahlenregisterbehörde, für die de facto eine halbe Person zur Verfügung steht, ist außerstande, diesen Arbeitsanfall innerhalb angemessener Zeit zu bewältigen.

Weiters sind in den von der EU-Kommission am 25. Jänner 2012 vorgelegten Vorschlägen zum neuen Rechtsrahmen im Datenschutz (Grundsatz-Verordnung und Richtlinie), die die Richtlinie 95/46/EG und den Rahmenbeschluss 2008/977/JI ablösen sollen, einheitliche Pflichten und Befugnisse der Datenschutzbehörden vorgesehen, die weit über die Aufgaben der Datenschutzkommission hinausgehen.

5.1.3 Beschwerden von Bürgern und Verfahren von Amts wegen

Mit dem derzeitigen Personalstand des Büros der Datenschutzkommission lassen sich, wie die statistischen Auswertungen im Abschnitt »Geschäftsgang« gezeigt haben, die (formellen) Beschwerdeverfahren einigermaßen bewältigen; bei entsprechend starker Anspannung ist es möglich, jene Verfahren, für die die gesetzliche Entscheidungspflicht des § 73 AVG gilt, grundsätzlich innerhalb von 6 Monaten durchzuführen.

Bei den Ombudsmannverfahren ist es im Berichtszeitraum allerdings keineswegs immer gelungen, eine Erledigungsdauer von weniger als 6 Monaten zu erreichen. Die Zahl dieser Verfahren nimmt stetig zu und kann daher selbst durch Überstundenleistung nicht mehr ausgeglichen werden. Zusätzliche Referenten/Referentinnen wären in diesem Bereich unbedingt erforderlich. Auch viele – von Amts wegen gebotene – Kontrollverfahren lassen sich wegen des Personalmangels nicht oder nicht in angemessener Zeit erledigen.

Ergänzend sei angemerkt, dass die (sich über das ganze Bundesgebiet erstreckenden) immer wieder notwendigen Einschauen – vor allem im Bereich der Videoüberwachung – mit dem vorhandenen Personal in keiner Weise bewerkstelligt werden können. Dafür müssten noch weitere Mitarbeiter und Mitarbeiterinnen aufgenommen werden, die entsprechende Dienstreisen zu absolvieren hätten.

Weiters hat sich im Berichtszeitraum das Problem der mangelnden Datensicherheitsmaßnahmen als besonderer Gegenstand von § 30-Verfahren herauskristallisiert. Dies betrifft vor allem jene Verfahren, die Hackerattacken auf Datenanwendungen und die – damit verbunden – die Meldung von Datenschutzverstößen (»Data Breach Notification«) betreffen. In diesem Zusammenhang, aber auch aufgrund des Fortschreitens komplexer Technologien hat es sich als besonderes Problem herausgestellt, dass die Datenschutzkommission nicht einmal über einen Mitarbeiter mit technischer Ausbildung verfügt. Nachdem sich die Beschwerden in Kontrollverfahren zunehmend neben der Videoüberwachung auf das Internet (inklusive Suchmaschinenproblematik und Soziale Netzwerke) fokussieren, ist die Arbeit ohne technisches Know-how praktisch nicht mehr zu bewältigen.

5.1.4 Zusammenarbeit auf EU-Ebene

Diesbezüglich hat sich die Situation gegenüber dem letzten Datenschutzbericht in keiner Weise geändert.

Es ist nach wie vor nur durch besondere Anstrengungen möglich, (wenn auch oft nur sehr oberflächlich) an den wichtigsten Aktivitäten der Art. 29 Gruppe und mancher ihrer Unterarbeitsgruppen sowie an den Sitzungen der Gemeinsamen Kontrollinstanzen der (ehemaligen) Dritten Säule (vgl. dazu Abschnitt 7) teilzunehmen. Die Beschickung einiger Unterarbeitsgruppen ist jedoch mangels Ressourcen gar nicht möglich.

Wie wichtig intensive Mitarbeit in diesem Bereich wäre, ergibt sich daraus, dass die wesentlichen datenschutzrechtlichen Herausforderungen heute regelmäßig nicht mehr auf die nationale Ebene beschränkt sind, sondern eine globale Dimension haben; es ergibt sich daher zwangsläufig, dass die Antworten auf diese Herausforderungen auf Ebene der Europäischen Union gesucht werden. Typische Beispiele hiefür sind etwa die zwingende Übermittlung von Flugpassagierdaten an Flugdestinationsländer (»PNR«), der Zugriff auf europäische Zahlungsverkehrsdaten im Zuge der Terrorismusbekämpfung (»SWIFT«) oder die Verwendung von personenbezogenen Daten in internationalen Konzernen (»BCRs«), aber auch grenzüberschreitende Datenschutzprobleme wie die Nutzung von Internetdiensten (wie z.B. »Google Street View«) oder sozialer Netzwerke wie »Facebook«. Überdies leistete die Datenschutzgruppe als Beratungsorgan der Europäischen Kommission kontinuierlich Beiträge im Zusammenhang mit der Erarbeitung der neuen Rechtsinstrumente im Datenschutz und wird auch in der weiteren Diskussion ihre Expertise zur Verfügung stellen. Auch für einen entsprechenden Informationsaustausch und zum Teil konzertierte Vorgangsweisen im Zusammenhang mit den in den Berichten Edwards Snowdens aufgezeigten Problemen mit der Praxis der US-Geheimdienste (NSA) stellte die Art. 29 Gruppe ein wertvolles Forum dar.

Daran zeigt sich, wie wichtig es auch für kleine Datenschutzbehörden wäre, sich entsprechend einbringen zu können.

Für diesen Tätigkeitsbereich gibt es nach wie vor keinen Referenten in der Geschäftsstelle der Datenschutzkommission, seitdem diese Planstelle mit 1.Juli 2006 verloren gegangen ist und die neue juristische Planstelle vorwiegend für die Bearbeitung von den – im Steigen begriffenen – Beschwerdeverfahren eingesetzt werden muss. Angesichts der unvermeidlichen Rück-

wirkungen der im Rahmen der Art. 29 Gruppe erarbeiteten Lösungen auf den Datenschutz in Österreich wird versucht, nach Möglichkeit Personalressourcen für die Teilnahme an wichtigen Initiativen dennoch frei zu machen – an eine kontinuierliche und strategische ausgerichtete Einflussnahme auf die Arbeit auf europäischer Ebene ist unter diesen Voraussetzungen jedoch nicht zu denken. Dieses Problem wird sich – im Falle der Beschlussfassung über die Datenschutz-Grundverordnung – erheblich verstärken, da eine sinnvolle Zusammenarbeit der Datenschutzbehörden – auch im Rahmen des so genannten »Kohärenzmechanismus« – ohne entsprechendes Personal im internationalen Bereich nicht gewährleistet ist.

5.1.5 Prüfung von Datenanwendungen

Was beim gegebenen Personalstand weiters nicht ausreichend wahrgenommen werden kann, ist die regelmäßige und planvolle Prüfung von Datenanwendungen vor Ort (vgl. § 30 Abs. 2 und 3 DSG 2000). In diesem Punkt weist die Tätigkeit der Datenschutzkommission bei einem europäischen Vergleich das größte Defizit im Verhältnis zur Tätigkeit anderer nationaler Kontrollstellen auf.

5.1.6 Öffentlichkeitsarbeit

a) Information der Öffentlichkeit in Datenschutzfragen

Die Datenschutzkommission und ihre Geschäftsstelle sind trotz dauernden Zeitmangels bemüht, so viel als möglich zu objektiver und sachgerechter Information der Öffentlichkeit in Datenschutzbelangen beizutragen.

Das GfM hat zu aktuellen Datenschutzfragen zahlreiche Interviews für die Medien gegeben.

Es wurden Vorträge bei Universitätsveranstaltungen, bei Seminaren im In- und Ausland, Konferenzen und Kongressen verschiedenster Fachrichtung gehalten, um den Stellenwert von Datenschutz in den unterschiedlichsten Bereichen zu verdeutlichen.

Die Datenschutzkommission hat im Berichtszeitpunkt auch besondere Anstrengungen unternommen, um ihren Web-Auftritt möglichst informativ und aktuell zu gestalten.

b) Zur Einbeziehung der Datenschutzkommission in das Begutachtungsverfahren für Gesetzesentwürfe:

Im Berichtszeitraum sind für den Datenschutz wesentliche Gesetzes- und Verordnungsentwürfe regelmäßig auch der Datenschutzkommission zur Stellungnahme im Begutachtungsverfahren zugeleitet worden.

Die Datenschutzkommission macht von der Möglichkeit zur Stellungnahme bei besonders wichtigen Entwürfen (ausnahmsweise auch im EU-Bereich im Hinblick auf öffentliche Konsultationen) regelmäßig Gebrauch, und zwar auch dann, wenn sie zur Teilnahme im Begutachtungsverfahren nicht ausdrücklich aufgefordert worden sein sollte. Die Datenschutzkommission hat im Berichtszeitraum zu einigen Gesetzes- und Verordnungsentwürfen Stellung genommen, wie etwa zum Entwurf eines Transparenzdatenbankgesetzes 2012 und zum Entwurf einer Änderung der Standard- und Musterverordnung. Auch im Zusammenhang mit den Verhandlungen des EU-Datenschutzpakets lieferte die Datenschutzkommission zu bestimmten Fragen laufend ihren Input.

5.1.7 Personal- und Budgetangelegenheiten

Trotz der grundsätzlich vom Bundeskanzleramt zugesagten Weiterservicierung der Datenschutzkommission in personellen und organisatorischen Angelegenheiten fallen im Zusammenhang mit der Ausgliederung aus dem Bundeskanzleramt Aufgaben an, für die keinerlei

zusätzliches Personal zur Verfügung steht (siehe Punkt 6). Es bedürfte daher besonders hinsichtlich der dienst- und budgetrechtlichen Fragen und damit verbundenen Tätigkeiten einer verstärkten Leitungsassistenz.

5.1.8 Zusammenfassung

In den nach Auffassung der Datenschutzkommission wahrzunehmenden Bereichen »Kontrollverfahren«, »Zusammenarbeit auf EU-Ebene« und »Organisatorische Angelegenheiten« besteht dringender Handlungsbedarf hinsichtlich der Personalausstattung der Datenschutzbehörde. Im DVR besteht Bedarf nach (weiteren) qualifizierten A- und B-Bediensteten. Hinzuweisen ist auch insbesondere auf die Stammzahlenregisterbehörde, die aufgrund neuer ihr zugeteilter Aufgaben außerstande ist, ihre Aufgaben zu erfüllen Die Datenschutzkommission hat nicht nur wiederholt in ihren vergangenen Datenschutzberichten auf ihre prekäre personelle Situation hingewiesen, sie hat auch – ebenso erfolglos – das Bundeskanzleramt und die politische Ebene umfassend über ihre Probleme informiert.

6 Zur organisatorischen Situation der Datenschutzkommission

6.1 Zur räumlichen Unterbringung der Geschäftsstelle der Datenschutzkommission

Die Geschäftsstelle der Datenschutzkommission seit 2009 zur Gänze am Standort Hohenstaufengasse untergebracht.

Dies hat zu einer wesentlichen Erleichterung der Koordination der Arbeit zwischen den einzelnen Organisationseinheiten des Geschäftsstelle geführt.

6.2 Zur rechtlichen und faktischen Unabhängigkeit der Datenschutzkommission

6.2.1 Rechtslage bis zum 1. Mai 2013

a. Die Mitglieder der Datenschutzkommission »üben diese Funktion neben ihnen sonst obliegenden beruflichen Tätigkeiten aus« – dies wurde durch die DSG-Novelle 2010 in § 36 Abs. 3a ausdrücklich festgelegt. Damit wurde klargestellt, dass vor allem auch die Funktion des GfM der Datenschutzkommission keine hauptberufliche Tätigkeit ist, sondern nur neben einem Hauptberuf – derzeit neben der Leitung der Geschäftsstelle der Datenschutzkommission – ausgeübt werden kann. Die Geschäftsstelle war als Abteilung im Bundeskanzleramt eingerichtet.
b. Gemäß des »alten« § 38 Abs. 2 DSG 2000 hatte der Bundeskanzler zur Unterstützung der Geschäftsführung der Datenschutzkommission die notwendige Sach- und Personalausstattung bereitzustellen. Diese Verpflichtung war so umgesetzt, dass der Bundeskanzler der Datenschutzkommission eine Abteilung im Bundeskanzleramt als Geschäftsstelle zur Verfügung stellte. Der Bundeskanzler war Dienstvorgesetzter der Bediensteten dieser Geschäftsstelle (vgl. § 37 Abs. 2 DSG 2000 idF vor der DSG-Novelle 2013).
c. Durch die Änderung des Bundes-Verfassunggesetzes mit der Novelle BGBl. I Nr. 2/2008, wurde eine neue generelle verfassungsrechtliche Grundlage für die Einrichtung weisungsfreier Verwaltungsbehörden geschaffen (Art. 20 Abs. 2 B-VG neu). Gleichzeitig wurde die bisherige spezielle verfassungsrechtliche Grundlage der Weisungsfreiheit der Mitglieder der Datenschutzkommission im § 37 DSG 2000 durch Aufhebung des Verfassungsrangs dieser Bestimmung beseitigt und die Datenschutzkommission dem generellen Regime des Art. 20 Abs. 2 B-VG für weisungsfreie Verwaltungsbehörden unterstellt. Art. 20 Abs. 2 B-VG (neu) enthält nunmehr ein ausdrückliches Unterrichtungsrecht des zuständigen Bundesministers gegenüber weisungsfreien Verwaltungsbehörden in seinem Ressortbereich.

In der DSG-Novelle 2010 hatte diese neue Rechtslage auch insofern Niederschlag gefunden, als ein Unterrichtungsrecht des Bundeskanzlers nunmehr ausdrücklich in § 38 Abs. 2 DSG 2000 festgeschrieben war: »Der Bundeskanzler hat das Recht, sich jederzeit über alle Gegenstände der Geschäftsführung der Datenschutzkommission beim Vorsitzenden und dem geschäftsführenden Mitglied zu unterrichten.«

Darüber hinaus sah die DSG-Novelle 2010 die Einrichtung eines weiteren Unterrichtungs- und Einsichtsrechts des Datenschutzrates vor: Gemäß § 41 Abs. 2 Z 4 wurde dem Datenschutzrat

das Recht eingeräumt, »von der Datenschutzkommission Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen«. Diese Bestimmung schien jedenfalls im Hinblick auf Art. 20 Abs. 2 B-VG als verfassungsrechtlich bedenklich. Formell war von dieser Bestimmung nicht Gebrauch gemacht worden. Vielmehr bestand und besteht eine informelle Zusammenarbeit mit dem Datenschutzrat, indem das geschäftsführende Mitglied an Sitzungen und Diskussionen des Datenschutzrates teilnimmt.

6.2.2 Das Urteil des EuGH in der Rechtssache C-614[10]

Art. 28 Abs. 1 der Datenschutz-Richtlinie (DSRL) sieht vor, dass die Mitgliedstaaten eine oder mehrere öffentliche Stellen beauftragen müssen, die die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet überwachen. Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit war.

Das im Jahre 2010 ergangene Urteil des EuGH C-518/07, in dem die rechtliche Stellung bestimmter deutscher Länder-Datenschutz-Kontrollstellen in Prüfung gezogen wurde, hat eine strenge Auslegung des Begriffs der »Tätigkeit in völliger Unabhängigkeit« ergeben, wonach z. B. die aus der organisatorischen Einordnung dieser Kontrollstellen in den Länder-Innenministerien erwachsende Aufsicht der Länder als unionsrechtswidrig befunden wurde. Generell wurde in diesem Urteil die durch die Verordnung 2001/45 geschaffene Institution des EDPS (Europäischer Datenschutzbeauftragter) als Maßstab für die adäquate Einrichtung einer Datenschutz-Kontrollbehörde bezeichnet.

Wie im vorigen Datenschutzbericht ausgeführt wurde, hatte die Europäische Kommission im Verfahren C-614/10 Klage beim EuGH gegen die Republik Österreich wegen mangelnder Unabhängigkeit der Datenschutzkommission eingebracht. Das Urteil in diesem Verfahren erging am 16. Oktober 2012. Wie der EuGH ausführte, war die Datenschutzkommission zwar insofern funktionell unabhängig, als ihre Mitglieder gemäß § 37 Abs. 1 DSG 2000 »in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden« sind. Doch reiche eine solche funktionelle ‚Unabhängigkeit für sich allein nicht aus, um diese Kontrollstelle vor jeder äußeren Einflussnahme zu bewahren. Zwischen dem GfM und dem Bundeskanzleramt bestehe ein Dienstverhältnis, die es dem Vorgesetzten des GfM ermögliche, dessen Tätigkeiten zu überwachen. Insoweit genüge der Hinweis, dass nicht ausgeschlossen werden kann, dass die Beurteilung durch den Vorgesetzten, mit der das dienstliche Fortkommen dieses Beamten gefördert werden soll, bei diesem zu einer Form von »vorauseilendem Gehorsam« führen kann. Die Datenschutzkommission sei aufgrund der Bindungen des GfM an das ihrer Kontrolle unterliegende politische Organ nicht über jeden Verdacht erhaben.

Weiters hielt der EuGH fest, dass das Personal der Geschäftsstelle der Datenschutzkommission aus Beamten des Bundeskanzleramts besteht und auch die Eingliederung der Geschäftsstelle in das Bundeskanzleramt nicht den Schluss zulässt, dass die Datenschutzkommission ihre Aufgaben frei von jedem Einfluss des Bundeskanzleramts wahrnehmen kann. Das der Geschäftsstelle zur Verfügung gestellte Personal bestehe aus Beamten des Bundeskanzleramtes, das über diese Beamten die Dienstaufsicht gemäß § 45 BDG 1979 ausübe. Eine solche Dienstaufsicht des Staates sei aber nicht mit dem Unabhängigkeitserfordernis in Art. 28 Abs. 1 UAbs. 2 DSRL vereinbar. Angesichts der Arbeitsbelastung einer für den Schutz personenbezogener Daten zuständigen Kontrollstelle sowie der Tatsache, dass die Mitglieder der Datenschutzkommission ihre Tätigkeit neben anderen beruflichen Tätigkeiten ausüben, wäre davon auszugehen, dass die Mitglieder bei der Ausübung ihres Amtes weitgehend auf die Unterstützung durch das ihnen zur Verfügung gestellte Personal angewiesen seien.

10 Siehe dazu EuGH 16. 12. 2012, Rs C-624/10, Kommission/Österreich

Auch das Unterrichtungsrecht des Bundeskanzlers sei dazu angetan, die Datenschutzkommission einem mittelbaren Einfluss seitens des Bundeskanzlers auszusetzen, der nicht mit dem Unabhängigkeitserfordernis vereinbar sei. Das Unterrichtungsrecht sei zum einen sehr weit gefasst, da es sich auf alle Gegenstände der Geschäftsführung erstrecke, und zum anderen unbedingt.

Aus all diesen Erwägungen habe die Republik Österreich gegen die Verpflichtungen aus Art. 28 Abs. 1 UAbs. 2 DSRL verstoßen.

6.2.3 Die DSG-Novelle 2013 und Neuerlassung der Geschäftsordnung der Datenschutzkommission

Als Reaktion auf das Urteil wurde vom österreichischen Gesetzgeber die DSG-Novelle 2013[11] erlassen, die mit 1. Mai 2013 in Kraft trat. In § 37 Abs. 2 DSG 2000 ist nunmehr vorgesehen, dass die Datenschutzkommission eine eigene Dienstbehörde und Personalstelle ist. Im Bundesfinanzgesetz ist die notwendige Sach- und Personalausstattung sicherzustellen. Die Bediensteten der Geschäftsstelle unterstehen nur den Weisungen des Vorsitzenden der Datenschutzkommission. Der Vorsitzende der Datenschutzkommission übt die Diensthoheit über die Bediensteten in der Geschäftsstelle aus. Der Verfassungsausschuss hat im Ausschussbericht[12] zu § 37 Abs.2 DSG 2000 idF der DSG-Novelle 2013 festgehalten, dass er davon ausgeht, dass der Vorsitzende der Datenschutzkommission seine dort angesprochenen Befugnisse auch auf das GfM der Datenschutzkommission übertragen kann. Die Datenschutzkommission hat ihre Geschäftsordnung dementsprechend neu beschossen und vorgesehen dass der Vorsitzende seine Weisungsbefugnis bezüglich der laufenden Geschäfte an das GfM übertragen kann.[13] Ebenso ist eine Delegationsbefugnis an das GfM hinsichtlich der Dienstaufsicht über die Mitarbeiter/innen der Geschäftsstelle vorgesehen.[14] Der Vorsitzende der Datenschutzkommission hat auch von diesen Delegationsrechten Gebrauch gemacht und sowohl die laufenden Geschäfte als auch die Dienstaufsichtsbefugnisse hinsichtlich der Mitarbeiter/innen der Geschäftsstelle (mit Ausnahme jener über die Leiterin der Geschäftsstelle, die ja identisch mit dem GfM ist) an das GfM delegiert.

In § 38 Abs. 2 DSG 2000 idF der DSG-Novelle 2013 ist festgelegt, dass das Unterrichtungsrecht des Bundeskanzlers in unionsrechtskonformer Auslegung des Art. 20 Abs. 2 nunmehr dahingehend eingeschränkt ist, dass der Vorsitzende der Datenschutzkommission dem Unterrichtungsrecht nur insofern zu entsprechen hat, als dies nicht der völligen Unabhängigkeit der Kontrollstelle iSd Art. 28 Abs. 1 UAbs. 2 DSRL widerspricht. Im Übrigen wurde das ausdrückliche Informations- und Einsichtsrecht des Datenschutzrates gestrichen.

In aufgrund der in § 61 Abs. 9 DSG 2000 idF der DSG-Novelle 2013 vorgesehenen Regelung wurden die in der Geschäftsstelle der Datenschutzkommission tätigen Bediensteten als Bedienstete der Datenschutzkommission übernommen.

6.2.4 Anmerkungen zur »faktischen« Unabhängigkeit der Datenschutzkommission

Trotz der oben beschriebenen rechtlichen Rahmenbedingungen ist die Datenschutzkommission vor allem aufgrund der oben beschriebenen Personalsituation mit faktischen Problemen hinsichtlich der unabhängigen Ausübung ihrer Aufgaben konfrontiert. Da die Datenschutzkommission anlässlich der Ausgliederung aus dem Bundeskanzleramt keinerlei weiteren Ressourcen zur Verfügung gestellt bekommen hat, ist sie auf die Weiterführung der Servisierung (in Personalangelegenheiten wie auch sonstigen sämtlichen Infrastrukturangelegenheiten) durch

11 BGBl I Nr 57/2013.
12 2245 BlgNR 24. GP 2.
13 § 7 Abs. 1 der Geschäftsordnung der Datenschutzkommission, Beschluss vom 30.April 2013.
14 § 7 Abs. 3 der Geschäftsordnung der Datenschutzkommission.

das Bundeskanzleramt (das hier quasi als »Dienstleister« agiert) angewiesen. Eine völlige Unabhängigkeit der Datenschutzbehörde setzt aber die Möglichkeit einer eigenständigen Personalverwaltung voraus.

7 Auswirkungen der Verwaltungsgerichtsbarkeits-Novelle 2012

7.1 Die Verwaltungsgerichtsbarkeits-Novelle 2012

Im Berichtszeitraum wurde die Verwaltungsgerichtsbarkeits-Novelle 2012 beschlossen. Diese sieht die Auflösung zahlreicher unabhängiger Behörden, so auch der Datenschutzkommission, vor.

Wie in den beiden letzten Datenschutzberichten ausgeführt, hat sich die Datenschutzkommission gegen ihre Auflösung ausgesprochen.

Zu dem unter Zl BKA-601.999/0001-V/1/2010 in Begutachtung versendeten Entwurf einer Verwaltungsgerichtsbarkeits-Novelle 2010, als deren Folge die Datenschutzkommission aufgelöst werden soll, hatte die Datenschutzkommission folgende Stellungnahme abgegeben:

»Durch Z 25 des Teils A der in Z 36 des Novellenentwurfes vorgesehenen »Anlage« soll die Datenschutzkommission aufgelöst werden.

Die Datenschutzkommission übt die Funktion einer nationalen Datenschutz-Kontrollstelle im Sinne des Art. 28 der RL 95/46 aus. In jedem Mitgliedsstaat der EU müssen eine oder mehrere solche Kontrollstelle(n) eingerichtet sein. Für Kontrollstellen nach Art. 28 besteht somit eine unionsrechtliche Bestandsgarantie. Da die österreichische Datenschutzkommission die einzige nationale Kontrollstelle im Sinne des Art. 28 ist, kann eine Auflösung der Datenschutzkommission nur stattfinden, wenn gleichzeitig dafür Vorsorge getroffen ist, dass die Aufgaben nach Art. 28 der RL von anderen Organen der Republik Österreich wahrgenommen werden. Dies wird in dem vorliegenden Novellenentwurf jedoch verabsäumt.

Keine der Kompetenzen der Datenschutzkommission kann unmittelbar aufgrund des vorliegenden Gesetzestextes auf die Verwaltungsgerichte übergehen, da die Fälle des Art. 130 Abs. 1 zur Gänze auf die Aufgaben der Datenschutzkommission unanwendbar sind: In keinem Fall entscheidet die Datenschutzkommission über die in Art. 130 Abs. 1 genannten Fälle, insbesondere auch nicht über »den Bescheid einer Verwaltungsbehörde« (Art. 130 Abs. 1 Z 1) oder »die Ausübung von unmittelbarer Befehls- oder Zwangsgewalt« (Art. 130 Abs. 1 Z 2). Allein der Umstand, dass sich die Aufgaben, für die die Verwaltungsgerichte eigentlich geschaffen werden sollen, in keinem einzigen Fall mit jenen der Datenschutzkommission decken, ist ein wesentliches Indiz dafür, dass der intendierte Kompetenzübergang offenbar nicht auf ideale Voraussetzungen beim Kompetenzempfänger trifft, da dieser vorrangig für andere Tätigkeiten eingerichtet ist.

Selbst wenn die Absicht bestehen sollte, diese Vorsorge durch entsprechende spätere einfachgesetzliche Regelungen (Art. 130 Abs. 2) noch zu treffen, stehen einer derartigen Übertragung der Kompetenzen der Datenschutzkommission auf die Verwaltungsgerichte grundsätzliche und unüberwindliche Hindernisse entgegen: Die Novelle geht davon aus, dass durch die Schaffung von Verwaltungsgerichten für bestehende Rechtsschutzkompetenzen von Verwaltungsorganen eine zweckmäßigere – und zumindest aufkommensneutrale – Gesamtlösung gefunden wird und gleichzeitig keine Lücken im Rechtsschutzsystem entstehen. Diese Wirkung kann im Falle des Übergangs der Kompetenzen der Datenschutzkommission auf Verwaltungsgerichte nicht erreicht werden, weil der weit überwiegende Teil der Kompetenzen der Datenschutzkommission nicht »gerichtsfähig« ist, handelt es sich doch großteils um informellen (kurativen) Rechtsschutz oder vorbeugenden Rechtsschutz durch Kontrolle von Datenanwendungen unabhängig vom Vorliegen von Beschwerden: Die Durchführung von Ombudsmann-Verfahren nach § 30 DSG 2000 ist ihrer Natur nach am ehesten mit der Tätigkeit der Volksanwaltschaft – ausgedehnt auf den gesamten privaten Bereich – zu vergleichen; die Kontrolle der Rechts-

und Ordnungsmäßigkeit von Datenanwendungen gleicht am ehesten der Rechtmäßigkeitskontrolle durch den Rechnungshof, freilich eingeschränkt auf Fragen des Datenschutzes, aber ausgedehnt auf den gesamten privaten Bereich; dem vorbeugenden Rechtsschutz dient auch das Registrierungsverfahren im Datenverarbeitungsregister.

»Gerichtsfähig« sind nur die förmlichen Entscheidungen der Datenschutzkommission in Verfahren nach § 31 DSG 2000, die in ihrem Gesamtaufwand jedoch bestenfalls 25 % des Gesamt-Arbeitsaufwands der Behörde »Datenschutzkommission« darstellen. Von diesen »gerichtsfähigen« Aufgaben ist der überwiegende Teil dennoch nicht an Verwaltungsgerichte übertragbar, da es sich nicht um Beschwerdefälle handelt, die ein Verhalten »in Vollziehung der Gesetze« (Art. 130 Abs. 2 Z 1) zum Gegenstand haben: Die Behandlung der Beschwerden wegen Verletzung im Recht auf Auskunft durch Auftraggeber des privaten Bereichs – die zahlenmäßig den weitaus größten Teil der Verfahren nach § 31 DSG 2000 ausmachen – ist nach dem vorliegenden Novellentext nicht auf Verwaltungsgerichte übertragbar, sodass im Endeffekt bestenfalls 10 % der Tätigkeit der Datenschutzkommission überhaupt für eine Übertragung (durch besonderes einfaches Gesetz) auf die Verwaltungsgerichte in Frage kämen. (Ein Eingehen auf die Frage, ob die Übertragung an das Bundesverwaltungsgericht oder teilweise an die Landesverwaltungsgerichte erfolgen müsste, scheint angesichts der Schwierigkeit der Einordnung des – derzeit noch geltenden – § 2 Abs. 2 DSG 2000 in den neuen Art. 131 im derzeitigen Stadium der Diskussion entbehrlich).

Daraus folgt, dass bei Auflösung der Datenschutzkommission eine neue Behörde geschaffen werden müsste, der der Löwenanteil der bisherigen Kompetenzen der Datenschutzkommission übertragen wird. Daraus folgt weiters, dass die Auflösung der Datenschutzkommission in keiner Weise zweckmäßig sein kann:

1. Zusätzlich zu den Verwaltungsgerichten müsste nach wie vor eine eigene Behörde als Datenschutz-Kontrollstelle mit umfangreichen Kompetenzen eingerichtet sein. Dies kann nicht aufkommensneutral oder gar einsparend wirken, da sich zumindest eine zusätzliche Behörde und damit zusätzliches Personal mit Fragen des Datenschutzes intensiv auseinandersetzen müsste. Auch würde dadurch die Einheitlichkeit der Rechtsprechung reduziert. Für die Wirtschaft ist aber jede Kompetenzzersplitterung ein zusätzlicher Kostenfaktor, da damit die Entscheidungen inhaltlich schwerer vorhersehbar werden.
2. Wenn die Beschwerden nach § 31 DSG 2000 über Auftraggeber des öffentlichen Bereichs tatsächlich an die Verwaltungsgerichte übertragen werden, weil die Datenschutz-Kontrollstelle keine gerichtsähnliche Tätigkeit entfalten soll, müssten parallel dazu die Beschwerden über Auskunftsverletzungen durch Auftraggeber des privaten Bereichs wieder an die ordentlichen Gerichte zurückfallen, die vor dem DSG 2000 hiefür zuständig waren. Dies würde eine entscheidende Einbuße für die Betroffenen im Rechtsschutzsystem zur Folge haben, da erfahrungsgemäß in Datenschutzsachen vom Rechtsschutz vor den ordentlichen Gerichten infolge des Prozessrisikos kaum Gebrauch gemacht wird. Es käme daher zu einer Verschlechterung der Gesamtsituation aus dem Blickwinkel eines effektiven Rechtsschutzes.
3. Der Verwaltungsgerichtshof würde durch den Übergang von Datenschutzkompetenzen auf die Verwaltungsgerichte in keiner Weise entlastet, da diese in erster Instanz entscheiden würden und daher der Rechtszug zum VwGH so wie bisher offenstehen muss.
4. Die Verwaltungsgerichte sind ihrer Natur nach nicht für Entscheidungen in erster Instanz und für die dafür notwendigen Sachverhaltsermittlungen gedacht, sodass übertragene Datenschutzkommissions-Kompetenzen zur Entscheidung in Beschwerdesachen jedenfalls einen Fremdkörper bei den Verwaltungsgerichten darstellen würden. Auch aus diesem Grund scheint die »Ersetzung« der Datenschutzkommission durch Verwaltungsgerichte zweckwidrig und völlig ungeeignet, in irgendeiner Weise Mehrwert zu erzeugen.

5. Im Übrigen darf darauf hingewiesen werden, dass die wiederholte öffentliche Ankündigung der Auflösung der nationalen Datenschutz-Kontrollstelle – ohne die geringste Erwähnung einer brauchbaren Alternativlösung – geeignet ist, im europäischen Kontext Befremden hervorzurufen und überdies die Arbeit der österreichischen Datenschutzkommission im nationalen wie im europäischen Zusammenhang zu behindern.

Überdies ist noch in Erinnerung zu rufen, dass sich die Prüfungsaufgabe der Datenschutzkommission über alle Bereiche des Verwaltungs- und Zivilrechts erstreckt und durch die derzeit vorgesehene Zusammensetzung der Datenschutzkommission auch gewährleistet ist, dass die Erfahrungen aus diesen Bereichen in die Entscheidungen der Datenschutzkommission einfließen können.«

Weiters wurde von der Datenschutzkommission im letzten Datenschutzbericht darauf hingewiesen, »dass in dem von der EU-Kommission am 25. Jänner 2012 vorgelegten Vorschlag für eine Datenschutz-Grundverordnung der Aufsichtsbehörde effektive Eingriffsbefugnisse wie die Anordnung der Löschung oder Berichtigung einer Datenanwendung eingeräumt werden, so dass es wohl kaum Sinn machen würde, derartige Befugnisse der Datenschutzkommission zu entziehen. Wenn die Kompetenzen der Kontrollstelle aber im Grunde nicht reduziert werden sollen und im Gegenteil in Zukunft eine Ausweitung der Befugnisse zu erwarten ist, stellt sich wiederum die Frage nach der Sinnhaftigkeit einer Auflösung der Datenschutzkommission. Ein Bundesverwaltungsgericht könnte sinnvoller Weise nur als zweite Instanz agieren (was im Übrigen mit zusätzlichen Kosten verbunden ist). Die geplante Auflösung der Datenschutzkommission sollte seitens der Gesetzgebung im Lichte der oben stehenden Ausführungen daher nochmals überdacht werden.«

Trotz dieser Bedenken der Datenschutzkommission hielt der Gesetzgeber daran fest, die Datenschutzkommission gemeinsam mit etwa 120 anderen Behörden mit 31. Dezember 2013 aufzulösen.

7.2 Die DSG-Novelle 2014[15]

Wenngleich eine Auflösung der Datenschutzkommission nicht zu verhindern war, entspricht die DSG-Novelle 2014 zumindest in einem wichtigen Punkt den Bedenken der Datenschutzkommission. Dies betrifft die Beibehaltung der bisherigen Aufgaben, vor allem der effektiven Eingriffsbefugnisse, wie sie insbesondere im formellen Beschwerdeverfahren gegeben sind.

Mit der DSG-Novelle 2014 wird mit 1.Jänner 2014 eine neue Datenschutzbehörde eingerichtet, die in Zukunft als Kontrollstelle iSd Art. 28 Abs. 1 DSRL agieren soll. An der Spitze der Behörde steht ein Leiter. Sowohl der Leiter als auch sein Stellvertreter werden vom Bundespräsidenten auf Vorschlag der Bundesregierung für fünf Jahre bestellt und können wiederbestellt werden.

Die Aufgaben der Datenschutzbehörde bleiben – wie oben erwähnt – im Wesentlichen dieselben wie jene der Datenschutzkommission. Die Datenschutzbehörde ist allerdings nun ausdrücklich vor Erlassung von Bundesgesetzen, die wesentliche Fragen des Datenschutzes unmittelbar betreffen, sowie von Verordnungen des Bundes, die auf der Grundlage dieses Bundesgesetzes

15 BGBl Nr 83/2013.

ergehen oder sonstige wesentliche Fragen des Datenschutzes unmittelbar betreffen, anzuhören. Weiters ist nunmehr von der Datenschutzbehörde ein jährlicher Jahresbericht zu erstellen.

Neu ist der nunmehr vorgesehene Rechtszug an das Bundesverwaltungsgericht: Sowohl Beschwerdeführer als auch Beschwerdegegner haben in Zukunft die Möglichkeit,, eine Beschwerde gegen einen Bescheid der Datenschutzbehörde an das Bundesverwaltungsgericht zu erheben. Bei Untätigkeit der Datenschutzbehörde können die Parteien Säumnisbeschwerde erheben; auch hiefür ist in Hinkunft das Bundesverwaltungsgericht zuständig.

Beim Bundesverwaltungsgericht wird über derartige Beschwerden ein Richtersenat bestehend aus einem Vorsitzenden (Berufsrichter) und zwei fachkundigen Laienrichtern aus dem Kreis der Arbeitgeber und aus dem Kreis der Arbeitnehmer entscheiden. Gegen deren Erkenntnisse ist – im Rahmen der verfahrensgesetzlich vorgesehenen Möglichkeiten – Revision an den Verwaltungsgerichtshof möglich.

Die bei der Datenschutzkommission anhängigen Verfahren werden ab 1. Jänner 2014 von der Datenschutzbehörde weitergeführt. Die Bediensteten der Datenschutzkommission werden von der Datenschutzbehörde ab 1. Jänner 2014 als Bedienstete der Datenschutzbehörde übernommen.

8 Zum Inhalt der im Berichtszeitraum durchgeführten Verfahren[16]

8.1 Beschwerdeverfahren nach § 1 Abs. 5 bzw.. § 31 DSG 2000

Gemäß § 1 Abs. 5 DSG 2000 ist die DSK zur förmlichen Rechtsdurchsetzung – d.h. zur Entscheidung über Datenschutz-Beschwerden in Bescheidform – berufen, soweit der öffentliche Bereich betroffen ist; im privaten Bereich sind grundsätzlich die ordentlichen Gerichte in Datenschutzsachen zuständig.

Nur hinsichtlich des Rechts auf Auskunft (§§ 1 Abs. 3 Z 1 und 26 DSG 2000) erstreckt sich die Zuständigkeit der DSK zur förmlichen Rechtsdurchsetzung auch auf den privaten Bereich.

8.1.1 Recht auf Auskunft

Als Folge der umfassenden Zuständigkeit der DSK zur förmlichen Durchsetzung des Auskunftsrechts machen Verfahren wegen Verletzung dieses Rechts den weitaus größten Teil der Beschwerdefälle aus.

Mit der DSG-Novelle 2010 wurde die DSK in die Lage versetzt, ein Verfahren wegen behaupteter Verletzung auf Auskunft formlos einzustellen, wenn die Rechtsverletzung beseitigt scheint und der Beschwerdeführer nicht binnen angemessener Frist begründet, warum die Rechtsverletzung zumindest teilweise als noch nicht beseitigt erachtet wird (§ 31 Abs. 8 DSG 2000). Wesensänderungen in der Sache durch die Äußerung bedeuten nun gesetzlich explizit eine konkludente Zurückziehung der ursprünglichen Beschwerde (die die formlose Einstellung des Beschwerdeverfahrens nach sich zieht) und gleichzeitiger Einbringung einer neuen Beschwerde (ebenda).

In diesem Bereich verdienen die folgenden, im Berichtszeitraum durchgeführten Verfahren besondere Erwähnung:

a. »Organisationsverschulden« bei Auskunft (K121.799/0008-DSK/2012, 27. 6. 2012)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass die Beschwerdegegnerin (eine Bildungseinrichtung) sein (in der Beschwerde näher dokumentiertes) Auskunftsbegehren aus Oktober 2011 nicht beantwortet habe. Die Beschwerdegegnerin hielt dem, rechtsanwaltlich vertreten, entgegen, der Beschwerdeführer sei ihr Angestellter in der IT und habe auch den Lehrgang zur Ausbildung als betrieblicher Datenschutzbeauftragter gemacht. Er sei selbst intern zum Schluss gekommen, er könne nicht bestimmen, welche auskunftspflichtigen Daten verarbeitet würden. Eine Beantwortung sei nicht möglich gewesen, weil weder der Vorgesetzte des Beschwerdeführers als für die Auskunftserteilung zuständiges Mitglied der Geschäftsführung noch der Beschwerdeführer selbst als IT-Administrator an der Auskunft mitgewirkt hätten. Die Beschwerdegegnerin sei daher außer Stande, die Auskunft zu erteilen.

Das Auskunftsschreiben wurde – unter Beifügung eines Identitätsnachweises – ordnungsgemäß zugestellt und bis zum Entscheidungszeitpunkt nicht beantwortet.

16 Sämtliche Entscheidungen sind abrufbar im Rechtsinformationssystem des Bundes (RIS) unter http://www.ris.bka.gv.at/dsb/

Rechtliche Würdigung:
Die Beschwerde erwies sich als berechtigt. Abgesehen davon, dass nicht einmal eine Negativauskunft erteilt wurde, sind organisatorische Besonderheiten (Auskunftsbegehren eines Mitarbeiters der IT-Abteilung), Unstimmigkeiten oder Zuständigkeitsstreitigkeiten innerhalb der Geschäftsführung oder eine zersplitterte Organisation der datenverarbeitenden Systeme keine tauglichen Rechtfertigungsgründe für die vollständige Verweigerung einer datenschutzrechtlichen Auskunft. Die Beschwerdegegnerin ist verpflichtet, ihre Struktur so zu gestalten, dass sie das Auskunftsrecht erfüllen kann.

Von einer Aufforderung zur Mitwirkung an den Beschwerdeführer gem § 26 Abs. 3 DSG 2000 zur Eingrenzung seines Auskunftsbegehrens (z. B. durch Identifizierung der infrage kommenden Datenanwendungen) wurde seitens der Beschwerdegegnerin kein Gebrauch gemacht.

Ebenfalls untauglich war der sinngemäße Einwand, der Beschwerdeführer hätte als Mitarbeiter der zentralen IT-Abteilung (mit den Nutzerprivilegien und Zugangsberechtigungen eines Systemadministrators) seine Daten gleichsam »in Selbstbedienung« suchen und finden können. Dem Gesetz ist, unabhängig von den tatsachenmäßigen Einwänden des Beschwerdeführers (kein Zugang zu allen Systemen), nämlich keinerlei derartige Einschränkung des Auskunftsrechts zu entnehmen.

Der Beschwerde war daher in vollem Umfang (als Leistungsauftrag an einen Auftraggeber des privaten Bereichs) Folge zu geben.

b. Auskunft bei intelligenten Wasserzählern (K121.822/0009-DSK/2012, 3. 8. 2012)

Sachverhalt:
Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass der Beschwerdegegner, ein Wasserleitungsverband, sein Auskunftsbegehren aus Jänner 2012 (betreffend Datenermittlung und technische Funktionen mithilfe eines neu installierten, per Funkverbindung zur Fernwartung und Fernablesung geeigneten Wasserzählers [vom Beschwerdeführer als »Smart Meter« bezeichnet]) nur unzureichend, nämlich unrichtig und unvollständig beantwortet habe. Es handle sich um einen »Feldversuch«, da es keine gesetzliche Verpflichtung für den Beschwerdegegner gebe, derartige »Smart-Meter«-Zähler zu installieren, über dessen datenschutzrechtlichen und funktechnischen Auswirkungen er nähere Informationen verlangt, aber nicht erhalten habe.

Der Beschwerdeführer ist Kunde des Beschwerdegegners, dem die Wasserversorgung des im Eigentum des Beschwerdeführers gelegenen Einfamilienhauses obliegt. Im Dezember 2011 wurde an dieser Adresse ein neuer Wasserzähler samt Funkmodul installiert. Dieser Sender (Leistung 10 mW) strahlt in kurzen Intervallen (7 bis 8 Sekunden) ein Einrichtungs-Funksignal aus, in dem Zählernummer (zur Identifikation des Kunden) und aktueller Zählerstand verschlüsselt sind. Mittels dieses Signals können die Daten im Nahbereich (rund 400 Meter im Umkreis) von einem Mitarbeiter oder Beauftragten des Beschwerdegegners mit einem mobilen Datenerfassungsgerät aufgefangen und verarbeitet werden (Drive-by- bzw. Walk-By-Datenerfassung).

Im Jänner 2012 richtete der Beschwerdeführer folgendes Auskunftsbegehren per E-Mail (unter Anschluss einer Reispasskopie als Identitätsnachweis) an den Beschwerdegegner:

»Zu diesem Wasserzähler habe [ich] nachstehende Fragen im Sinne des Datenschutzgesetzes und ersuche um schriftliche Beantwortung an folgende Adresse [...]:

- Unter welcher DVR Nr. wurde durch den Wasserleitungsverband diese neue Art der personenbezogenen Datensammlung an die Datenschutzkommission gemeldet[?] Es besteht dazu eine gesetzliche Meldepflicht welche bei Nichteinhaltung mit Strafe bedroht ist. Ich ersuche um Zusendung einer Kopie dieser Meldung.
- Liegt für diese »Funkgeräte« eine funkrechtliche Genehmigung der Fernmeldebehörde vor, Bitte um eine Kopie[?]
- Können Gesundheitsschädigungen durch diesen ‚Funkverkehr' ausgeschlossen werden, Bitte um eine Kopie der Testberichte[?]
- Welche Daten ‚genau' werden mittels diesem Gerät auf welcher Funkfrequenz ausgelesen?
- Wird der jeweilige Hausbesitzer und Kunde jedesmal über die durchgeführte Auslesung informiert?
- Welche IKT-Sicherheitstest[s] wurden durchgeführt um eine Manipulation über Funk zu verhindern?
- Welche IKT-Sicherheitstest[s] wurden durchgeführt um eine ‚hacken' dieses Geräts zu verhindern?
- Ist dieser neue bei mir eingebaute Wasserzähler im österreichischen EICHGESETZ verankert?

Weiters ersuche ich um Zusendung einer genauen Betriebsanleitung und Beschreibung dieses Geräts soweit dies möglich ist, da es im Internet und auf ihrer Website so gut wie keine Informationen dazu gibt.

Ich ersuche um sorgfältige Behandlung meiner Anfrage im Sinne des gültigen Datenschutzgesetzes.«

Der Beschwerdegegner erteilte dem Beschwerdeführer mit Schreiben aus Jänner 2012 fristgerecht Auskunft. Neben Angaben zu den technischen Daten des Funkmoduls wurde dem Beschwerdeführer die DVR-Nummer des Beschwerdegegners sowie die Negativauskunft übermittelt, dass mittels des neuen Wasserzählers samt Funkmodul

- keine personenbezogenen Daten übermittelt werden und
- die Datenmenge gegenüber der früheren Ablesung der alten Zähler durch ein Zählorgan unverändert geblieben sei (Ablesung einmal jährlich).

Im Februar 2012 wurde die vorliegende Beschwerde (wegen inhaltlicher Mängel dieser Auskunft) eingebracht. Im März 2012 erteilte der Beschwerdegegner dem Beschwerdeführer im laufenden Verfahren eine »Richtigstellung« der Auskunft bzw. eine ergänzende Auskunft.

Diese bestand hinsichtlich der verarbeiteten Daten insb aus Screenshots mit den Daten des seit 2003 zur Verrechnung in Verwendung stehenden EDV-Programms. Aus diesen ging hervor, dass der neue Zähler im Oktober 2011 bei Zählerstand »1« anlässlich des Einbaus und Ende Oktober 2011 bei einer »Turnusablesung« (eine solche erfolgte auch in den Vorjahren stets gegen Ende des Kalendermonats Oktober) mit Zählerstand »10« ausgelesen und die entsprechenden Daten mit Bezug zum Beschwerdeführer (als »Geschäftspartner« zusammen mit einer weiteren Person) verarbeitet wurden. Zur Datenherkunft wurde wörtlich ausgeführt: »Weiters werden periodisch (jährlich) die Zählerstände des Wasserzählers der Anlage [...] samt dazugehöriger Wasserzählernummer durch Funkfernablese bzw. früher durch Ablese des Zählerstandes durch Dienstnehmer des WLV erhoben. Im Rahmen der Funkfernablese werden ausschließlich der Zählerstand sowie die Wasserzählernummer ausgelesen und übermittelt.«

Rechtliche Würdigung:
Die Beschwerde hat sich als unbegründet erwiesen.

Von dem vom Beschwerdeführer an den Beschwerdegegner gerichteten Fragen fallen überhaupt nur die erste und die vierte in den Anwendungsbereich des DSG 2000 und nur die vierte unter das Auskunftsrecht gem § 26 Abs. 1 DSG 2000. Alle anderen stellen Fragen allgemeiner und technischer Natur dar, deren Beantwortung nicht im Beschwerdeverfahren nach § 31 Abs. 1 DSG 2000 durch die Datenschutzkommission erzwungen werden kann.

Die Herstellung von Datensicherheit gem § 14 DSG 2000 ist eine Pflicht des datenschutzrechtlichen Auftraggebers, deren mögliche Missachtung aber in einem Beschwerdeverfahren wegen Verletzung des Auskunftsrechts nicht näher zu prüfen ist. Eine Beschwerde wegen Verletzung des Auskunftsrechts bietet auch keinen rechtlichen Grund oder Anlass, die Frage der Zulässigkeit des Einsatzes von sogenannten »Smart-Meter«-Messgeräten zu prüfen und zu erörtern.

Das Datenverarbeitungsregister (DVR) ist ein von der Datenschutzkommission geführtes öffentliches Register. Im Ausgleich zur Meldepflicht, die einen datenschutzrechtlichen Auftraggeber treffen kann, ist letzterer nicht verpflichtet, Informationen, die sich jedermann durch Einsichtnahme ins DVR beschaffen kann (einschließlich der möglichen Information, dass eine Datenanwendung nicht gemeldet und registriert worden ist), in eine Auskunft gem § 26 Abs. 1 und 4 DSG 2000 einzubeziehen. Gegenstand einer solchen Auskunft sind die nicht öffentlich einsehbaren, dem Datengeheimnis unterliegenden Inhalte einer Datenanwendung. Durch die Nicht-Übermittlung einer Kopie der DVR-Meldung des Beschwerdegegners kann der Beschwerdeführer auch nicht in seinem Recht auf Auskunft über eigene Daten verletzt worden sein, da die im DVR verarbeiteten Daten den jeweiligen Auftraggeber, hier also den Beschwerdegegner, betreffen. Es handelt sich inhaltlich um die »Angaben«, dass der betreffende Auftraggeber die genannten Datenarten der umschriebenen Betroffenenkreise verarbeitet (und evtl an weitere Auftraggeber, umschrieben als Empfänger oder Empfängerkreise, übermittelt).

Dem Beschwerdeführer ist es nicht gelungen, die Unrichtigkeit der im Jänner 2012 erteilten und im März 2012 ergänzten Auskunft darzulegen.

Es trifft zu, dass die ursprüngliche Auskunft als Negativauskunft nicht dem Gesetz entsprochen hat, da der Beschwerdegegner, auch mithilfe des Zählers, Daten über den Beschwerdeführer verarbeitet. Der Beschwerdegegner hat jedoch von der ihm gesetzlich in § 31 Abs. 8 DSG 2000 eingeräumten Option Gebrauch gemacht, die Auskunftserteilung durch Ergänzungen zu sanieren und die Verletzung im Auskunftsrecht damit zu beseitigen, den Beschwerdeführer also »klaglos zu stellen«.

Die vom Beschwerdeführer dazu nach Parteiengehör gemachten Einwände waren nicht stichhaltig. Bezüglich des Hinweises auf die Diskrepanz zwischen dem Intervall des abgestrahlten Funksignals und den Zeitpunkten der Datenerfassung ist zu sagen, dass nur im Zeitpunkt der Auslesung des Zählers, dh der Erfassung und dauerhaften Speicherung des per Funk abgestrahlten Zählerstandes durch den Beschwerdegegner, ein relevanter Verarbeitungsschritt erfolgt. Auf die Häufigkeit der Ausstrahlung des (nicht erfassten) verschlüsselten Funksignals kommt es hingegen nicht an, da über nicht verarbeitete Daten auch keine Auskunft zu erteilen ist.

Die Beschwerde war daher spruchgemäß als unbegründet abzuweisen.

c. Grenzen der Auskunft durch eine Bezirkshauptmannschaft (K121.908/0003-DSK/2013, 20.2. 2013)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass die in Beantwortung seines Auskunftsbegehrens aus Juli 2012 erteilte Auskunft unvollständig sei. Er habe keine Datenauszüge erhalten. Weiters seien ihm, trotz eines entsprechenden Ersuchens, die Datenanwendungen der Beschwerdegegnerin (eine Bezirkshauptmannschaft) nicht bekannt gegeben worden. Überdies habe die PAD-Auskunft statt eines österreichweiten PAD-Auszuges nur Daten aus dem Bezirk enthalten. Zuletzt fehlten Daten aus bestimmten Datenanwendungen und ein »Verwaltungsstrafregisterauszug« aus der Verwaltungsstrafevidenz der Beschwerdegegnerin.

Die Beschwerdegegnerin hat den Beschwerdeführer auf sein allgemein formuliertes Auskunftsbegehren gem § 26 Abs. 3 DSG 2000 zur Mitwirkung aufgefordert. Daraufhin ersuchte der Beschwerdeführer um Bekanntgabe der von der Beschwerdegegnerin betriebenen Datenanwendungen. In der Folge erteilte die Beschwerdegegnerin Auskunft aus dem Kriminalpolizeilichen Aktenindex (KPA), der Aktenverwaltung PAD (betreffend »Organisationseinheiten, die ihr zuzurechnen sind) sowie aus der Anwendung »Verwaltungsstrafen«.

Rechtliche Würdigung:

A. Die Beschwerdegegnerin hat den Beschwerdeführer zu Recht unter Hinweis auf die Mitwirkungsobliegenheit gem § 26 Abs. 3 DSG 2000 zur Angabe von Datenanwendungen aufgefordert, aus denen im Einzelnen Auskunft gewünscht wird. Danach hat der Beschwerdeführer sein Auskunftsbegehren auf PAD, den KPA und die von der Beschwerdegegnerin geführte Verwaltungsstrafevidenz (gem § 60 SPG) eingeschränkt. Die Auskunftserteilung aus anderen Datenanwendungen, die erstmals in der Beschwerde erwähnt werden, war daher nicht Gegenstand dieser Beschwerdesache, bzw. des Auskunftsbegehrens.

Informationen über den Stand des Datenverarbeitungsregisters (DVR) sind nicht Gegenstand des durch § 26 DSG 2000 näher geregelten, subjektiven, gegenüber einem datenschutzrechtlichen Auftraggeber geltend zu machenden Auskunftsrechts. Die »Publizität der Datenanwendungen« (Abschnittsüberschrift vor § 16 DSG 2000) ist vielmehr durch den öffentlichen Zugang zum DVR (seit 1. September 2012 online über das Internet möglich) sichergestellt. Die Beschwerdegegnerin hat daher die Erteilung einer Auskunft über die von ihr durchgeführten Datenanwendungen insoweit begründet abgelehnt und auf das DVR verwiesen.

B. Kern der Beschwerde ist das Vorbringen des Beschwerdeführers, keine »Datenauszüge« (aus dem KPA, PAD bzw. der Verwaltungsstrafevidenz) erhalten zu haben. Das Gesetz definiert diesen Begriff allerdings nicht und räumt auch keinen entsprechenden Anspruch ein. Unzutreffend ist jedenfalls die Ansicht, dass im Zuge einer Auskunftserteilung ein »Original-Ausdruck« in einer bestimmten Form oder in einem bestimmten Daten oder Druckformat an den Auskunftswerber übermittelt werden muss. Das Gesetz legt in § 26 Abs. 1 und 4 DSG 2000 nur die Schriftform fest (mit der dem datenschutzrechtlichen Auftraggeber eingeräumten Möglichkeit, ein Auskunftsbegehren auch durch Gewährung von Einsicht zu erfüllen).

Das Recht, als Partei in einen von einer Sicherheitsbehörde geführten Verwaltungsakt (der Begriff steht hier für die schriftliche Dokumentation eines Verwaltungsverfahrens) Einsicht zu nehmen bzw. eine Aktenkopie zu erhalten (§ 17 AVG, §§ 51 bis 54 StPO), ist nicht mit dem datenschutzrechtlichen Auskunftsrecht gleichzusetzen. Das Datenschutzgesetz verleiht kein subjektives, vor der Datenschutzkommission geltend zu machendes Recht auf Akteneinsicht (Bescheid der Datenschutzkommission vom 4. Juni 2002, GZ: K120.810/005-DSK/2002).

Die Beschwerdegegnerin hat gegenüber dem Beschwerdeführer auch begründet, warum keine »Datenauszüge« vorgelegt werden müssen. Durch die Auskunftserteilung in gegebener Schriftform hat die Beschwerdegegnerin den Beschwerdeführer daher nicht im Recht auf Auskunft verletzt.

C. Das elektronische System »PAD« ist ein Aktenprotokollierungssystem (Aktenindex), das in der neueren Version »PAD 2.0« zusätzlich mit einem elektronischen Aktenbearbeitungs- und Aktenaufbewahrungssystem verbunden ist. Rechtsgrundlage für PAD ist § 13 Abs. 2 SPG. Diese Bestimmung ermächtigt nur die – trotz des Namens zu den Bundesbehörden zählenden – Landespolizeidirektionen (vormals die Sicherheitsdirektionen und die Bundespolizeidirektionen) in Angelegenheiten der Sicherheitsverwaltung, sich für Zwecke der Aktenprotokollierung und Verfahrensdokumentation eines derartigen Systems zu bedienen. Soweit Dienststellen der Bundespolizei PAD im Bereich der Vollziehung des SPG (sowie bei kriminalpolizeilicher Tätigkeit gem StPO) benützen, ist daher die Landespolizeidirektion als datenschutzrechtlicher Auftraggeber anzusehen. Soweit PAD funktionell auch andere Verwaltungsaufgaben einbezieht, muss im Einzelfall geprüft werden, welche Behörde als datenschutzrechtlicher Auftraggeber infrage kommt.

Für den Beschwerdeführer war daraus aber nichts zu gewinnen, da eine auftraggeberische Verantwortung der Beschwerdegegnerin und damit eine Auskunftspflicht für Daten, die von Polizeiorganen und -dienststellen außerhalb ihres Zuständigkeitsbereichs (laut Anlage zum Gesetz über die Organisation der staatlichen Bezirksverwaltung, LGBl. Nr. 1/1976 idgF) verarbeitet werden (der Beschwerdeführer begehrte wörtlich einen »österreichweiten PAD-Datenauszug«), jedenfalls nicht besteht.

Im eigenen Zuständigkeitsbereich wurde von der Beschwerdegegnerin auch inhaltlich Auskunft über den Beschwerdeführer betreffende PAD-Daten erteilt. Die Beschwerdegegnerin hat eine über die erteilte Auskunft hinausgehende Auskunftserteilung aus PAD daher zu Recht abgelehnt.

D. Hinsichtlich der Verwaltungsstrafevidenz übersieht der Beschwerdeführer, dass ihm im Auskunftsschreiben vom August 2012 sehr wohl eine Auskunft durch die Beschwerdegegnerin erteilt worden ist, nämlich eine Negativauskunft betreffend die »Anwendung Verwaltungsstrafen (VWS)«. Gegen den Inhalt dieser Auskunft ist nichts vorgebracht worden. Von dieser allgemeinen Evidenz der erfolgten Bestrafungen (gegründet u. a. auf die allgemeine Zuständigkeit der Bezirksverwaltungsbehörde in Verwaltungsstrafsachen gem § 26 Abs. 1 VStG) ist die Ermächtigung zur Führung einer besonderen Verwaltungsstrafevidenz gem § 60 SPG zu unterscheiden. Letztere betrifft nur Daten zu Strafen wegen der Verwaltungsübertretungen nach §§ 81 bis 84 SPG und ist gem § 60 Abs. 1 SPG von der Landespolizeidirektion (früher: der Sicherheitsdirektion) zu führen. Die Beschwerdegegnerin hat den Beschwerdeführer diesbezüglich zu Recht an diesen datenschutzrechtlichen Auftraggeber verwiesen.

d. Auskunft zur Registerzählung (K121.921/0007-DSK/2013, 10.4. 2013)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass die Beschwerdegegnerin (die Bundesanstalt Statistik Österreich) nicht über sämtliche Erhebungsmerkmale, die sie im Zusammenhang mit der Registerzählung ihn betreffend verarbeite, Auskunft erteilt habe. Er sei gem § 5 Abs. 5 RegzG von der Beschwerdegegnerin identifiziert worden. Somit sei ein Personenbezug zwischen dem »bereichsspezifischen Personenkennzeichen Amtliche Statistik« (kurz: bPK-AS) und Name und Adresse des Beschwerdeführers hergestellt worden. Auf diese Weise sei das bPK-AS hinsichtlich des Beschwerdeführers zu einem unmittelbar personenbezogenen Datum geworden, das zu beauskunften sei. Dies habe die

Beschwerdegegnerin jedoch, trotz ausdrücklichen Auskunftsbegehrens, unter Hinweis auf die Unmöglichkeit der Auskunftserteilung verweigert. Das bPK-AS sei bereits gelöscht worden. Diese Begründung erscheine dem Beschwerdeführer wegen der Bestimmungen der §§ 4 Abs. 1 und 6 Abs. 2 2. Satz RegzG nicht überzeugend. Weiters seien die Angaben der Beschwerdegegnerin in Bezug auf gem § 5 Abs. 6 RegzG gemachte Datenübermittlungen widersprüchlich, und es fehlten klare Angaben in Bezug auf den Betrieb von Standardanwendungen und die darin verarbeiteten Daten des Beschwerdeführers. Zuletzt führe die Beschwerdegegnerin keinen Grund an, warum eine Identifikation des Beschwerdeführers gem § 5 Abs. 5 RegzG durchgeführt worden sei. »Die vom Antragsgegner beauskunfteten Daten scheinen allerdings weder unvollständig noch widersprüchlich wie dies gem. § 5 Abs. 2 und 3 Registerzählungsgesetz für eine Identifikation des Antragstellers gefordert wäre und geben keinen Grund zum Anlass am Hauptwohnsitz des Antragsgegners zu zweifeln. Qualifiziert doch der Antragsgegner selbst die Adresse des Antragstellers als dessen Hauptwohnsitz. Dies sorgt für die Vermutung, dass der Antragsgegner eine unvollständige nicht den gesetzlichen Anforderungen entsprechende Auskunft erteilt hat.« Der Beschwerdeführer stellte den Antrag, der Beschwerdegegnerin die Erteilung einer vollständigen und gesetzeskonformen Auskunft durch Bescheid aufzutragen.

Der Beschwerdeführer ist mit einem Hauptwohnsitz in Österreich gemeldet, entsprechende Daten sind im örtlichen und im zentralen Melderegister verarbeitet. Dies galt auch für den 31. Oktober 2011 (Stichtag für die Volkszählung). Im Zuge der Volkszählung 2011, die erstmals als Registerzählung durchgeführt wurde, wurden diese Daten, ohne den Namen des Beschwerdeführers aber durch Verwendung des verschlüsselten bPK des Verwaltungsgebiets Meldewesen und des bPK-AS identifizierbar, vom Bundesministerium für Inneres als Basisdaten der Registerzählung an die Beschwerdegegnerin übermittelt.

Bei der Überprüfung für Zwecke der Qualitätssicherung wurde festgestellt, dass den Meldedaten des Hauptwohnsitzes des Beschwerdeführers keine weiteren Verwaltungsdaten zugeordnet werden konnten. Die Beschwerdegegnerin veranlasste daher die Identifizierung des Beschwerdeführers mithilfe des verwendeten bPK-AS und erhielt so den zum Meldedatensatz gehörigen Namen. Darauf wurde der Beschwerdeführer mit Schreiben aus Jänner 2012 von der Beschwerdegegnerin brieflich kontaktiert und um Angaben zum Bestehen des Hauptwohnsitzes ersucht.

Im Februar 2012 ersuchte der Beschwerdeführer die Beschwerdegegnerin gem § 26 Abs. 1 DSG 2000 um Auskunft. Dabei wurde insb um die Bekanntgabe des bPK-AS sowie sämtlicher weiterer bPKs, die zum Antragsteller gespeichert sind, und sämtlicher Daten, die mit dem bPK-AS verknüpft sind, darunter vor allem die im Rahmen der Registerzählung verarbeiteten Daten, ersucht. »Gemäß § 5 Abs. 5 Registerzählungsgesetz wurde Ihnen die Identität des Antragstellers zu den bei Ihnen im Rahmen der Registerzählung und mittels bPK-AS verknüpften Daten bekannt gegeben. Das bPK-AS des Antragstellers sowie sämtliche mit diesem, für jede Person eindeutigen, Personenkennzeichen verknüpften Daten stellen daher personenbezogene Daten gemäß § 4 Z 1 DSG 2000 dar und sind gemäß § 26 DSG 2000 zu beauskunften.«

Mit Schreiben aus April 2012 erteilte die Beschwerdegegnerin dem Beschwerdeführer eine datenschutzrechtliche Auskunft, die folgende relevante Passagen enthielt:

»[...] Zur Frage: Woher stammen die Daten, die Sie im Zusammenhang mit dem Antragsteller verarbeiten? Angabe jener Stellen, von denen Daten stammen.

Gemäß § 5 Abs. 4 Ziffer 3 Registerzählungsgesetz hat die Bundesanstalt zum Zweck der Wohnsitzanalyse eine Befragung der Betroffenen durchzuführen. Zu diesem Zweck wurde für das bPK-AS des Antragstellers der Familienname, Vorname sowie die aktuelle Wohnad-

resse vom Zentralen Melderegister zur Durchführung einer Befragung gemäß § 5 Registerzählungsgesetz angefordert.

Zur Frage: An wen wurden personenbezogene Daten des Antragstellers übermittelt?

An das Zentrale Melderegister wurden die verschlüsselten bPK-AS und bPK-ZP zur Bekanntgabe des Namens und der Adresse des Antragstellers gemäß § 5 Abs. 5 Registerzählungsgesetz übermittelt.[...]

Die Bundesanstalt hat gemäß § 1 Abs. 1 Registerzählungsgesetz zum Stichtag 31. Oktober 2011 eine Volks-, Arbeitsstätten-, Gebäude- und Wohnungszählung durchzuführen. Zudem hat die Bundesanstalt Statistik Österreich gemäß § 7 Registerzählungsgesetz innerhalb eines Jahres nach der letzten Datenlieferung die Zahl der zum Stichtag 31. Oktober 2011 mit Hauptwohnsitz in Österreich, in den Ländern, Regionalwahlkreisen (§ 3 NRWO), politischen Bezirken, Gemeinden und Wiener Gemeindebezirken lebenden österreichischen und nicht österreichischen Staatsbürgern unter Berücksichtigung der Ergebnisse der Qualitätssicherungsmaßnahmen gemäß § 5 Registerzählungsgesetz festzustellen.

Ist zweifelhaft, ob zum Stichtag ein Wohnsitz im Bundesgebiet noch aufrecht ist, hat die Bundesanstalt zum Zweck der Wohnsitzanalyse eine Befragung des Betroffenen durchzuführen. Die Betroffenen sind der Bundesanstalt gemäß § 5 Abs. 5 Registerzählungsgesetz zur zweckdienlichen Auskunftserteilung verpflichtet. Die Befragung, ob jemand in Österreich gemäß der Definition des Meldegesetzes einen Hauptwohnsitz zum Stichtag 31. Oktober 2011 hatte, ist eine derartige zweckdienliche und zudem die einzige Anfrage an den Betroffenen und damit das gelindeste Mittel, um festzustellen, ob eine Person im Inland zur Wohnbevölkerung zählt oder nicht.

Da die bereichsspezifischen Personenkennzeichen des Antragstellers nach Erhalt des Namens und der Adresse des Antragstellers durch das Zentrale Melderegister von der Bundesanstalt sofort gelöscht wurden, gibt es keine Möglichkeit, zum bereichsspezifischen Personenkennzeichen personenbezogene Auskünfte zu erteilen und die bereichsspezifischen Personenkennzeichen zum Antragsteller bekanntzugeben.[...]«

Rechtliche Würdigung:
Dem Beschwerdeführer war es nicht gelungen, gesetzwidrige Mängel in der erteilten Auskunft aufzuzeigen. So liegt kein Beweis dafür vor, dass die Beschwerdegegnerin das bPK-AS, mit dessen Hilfe die Meldedaten identifiziert wurden, verknüpft mit diesen Meldedaten verarbeitet.

Aus dem Verweis auf die im Datenverarbeitungsregister eingetragene Meldung einer Datenanwendung für Zwecke der gesetzlich angeordneten Registerzählung (DAN: 0000043/119 Registerzählung – Aufarbeitung nach § 5 Registerzählungsgesetz, BGBl. I Nr. 33/2006), die tatsächlich eine personenbezogene Verwendung des bPK-AS vorsieht, war für den Standpunkt des Beschwerdeführers nichts zu gewinnen. Der gemeldete Inhalt einer Datenanwendung bildet nur die äußere Grenze des regelmäßigen Umfangs der Verwendung personenbezogener Daten für einen bestimmten Zweck. Die registrierte Meldung ist weder konstitutiv für das Recht, die entsprechenden Daten zu verwenden, noch bildet sie einen Beweis, dass der Auftraggeber Daten eines bestimmten Betroffenen zu allen gemeldeten Datenarten verarbeitet.

Im Fall der Daten des Beschwerdeführers bezieht sich die personenbezogene Verwendung des bPK-AS nur auf den (kurzen) Zeitabschnitt von der (Rück-) Übermittlung der bPK an das ZMR und dem Erhalt des Namens des Beschwerdeführers. Für das weitere Befragungsverfahren wurde eine behördenübliche Geschäfts-/Ordnungszahl verwendet.

Aus dem Satz »Die Bundesanstalt hat die bPK-AS und die verschlüsselten bPK des betroffenen Tätigkeitsbereiches für Zählungen nach diesem Bundesgesetz sowie für andere statistische Erhebungen gemäß § 4 Abs. 1 des Bundesstatistikgesetzes 2000 aufzubewahren.« in § 6 Abs. 2 RegzG ist nicht der Schluss zu ziehen, dass diese Kennzeichen verknüpft mit dem Namen einer bestimmten Person abgespeichert werden dürfen. Die namentliche Identifizierung eines von der Registerzählung Betroffenen unter personenbezogener Verarbeitung des bPK-AS durfte im hier relevanten Sachverhalt vielmehr nur ausnahmsweise, zur Abklärung von Bedenken hinsichtlich der statistischen Qualität der Daten im Verfahren nach § 5 Abs. 2 bis 5 RegzG und zeitlich begrenzt erfolgen.

Diesbezüglich waren die Angaben der Beschwerdegegnerin daher glaubwürdig.

Es ist zwar richtig, wenn der Beschwerdeführer vorbrachte, dass dieser Identifizierungsvorgang rein technisch-administrativ wiederholt werden könnte. Er übersieht dabei aber, dass dies kein erlaubter, von einer gesetzlichen Ermächtigung gedeckter Vorgang wäre. Insofern steht der Beschwerdegegnerin kein rechtlich zulässiges Mittel zur Verfügung, um den direkten Personenbezug zwischen dem Beschwerdeführer und dem verwendeten bPK-AS neuerlich herzustellen. Das bPK-AS ist so für die Beschwerdegegnerin derzeit nur ein indirekt personenbezogenes Datum, das sie aufgrund ausdrücklicher gesetzlicher Anordnung weiter zu speichern hat.

Als indirekt personenbezogenes Datum unterliegt das bPK-AS aber gem § 29 DSG 2000 nicht dem Recht auf Auskunft. Die Beschwerdegegnerin hat die Auskunftserteilung damit hinsichtlich des bPK-AS mit zutreffenden Gründen abgelehnt.

Hinsichtlich der Standardanwendungen hat die Beschwerdegegnerin eine Negativauskunft erteilt. Der Beschwerdeführer hat, außer allgemein formulierten Zweifeln, nichts vorgebracht, was diesen Angaben widersprechen könnte.

Was das Vorbringen angeht, die Angaben der Beschwerdegegnerin zu den Gründen des Qualitätssicherungsverfahrens (Erhebungen zum Bestehen eines Hauptwohnsitzes) seien unzureichend, so übersieht der Beschwerdeführer, dass eine Beschwerde wegen Verletzung des Rechts auf Auskunft nicht zum Gegenstand hat, einen denkmöglichen Eingriff in das Recht auf Geheimhaltung zu überprüfen. Im Sinne des § 26 Abs. 1 DSG 2000 hat die Beschwerdegegnerin die Rechtsgrundlagen, auf die sie sich dabei berufen hat, jedenfalls korrekt angegeben.

Die Beschwerde war daher als unbegründet abzuweisen.

e. Rechtmäßige Reaktion auf ein Auskunftsbegehren (K121.924/0006-DSK/2013, 10.4. 2013)

Sachverhalt:
Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft über eigene Daten dadurch, dass der Beschwerdegegner (eine Bezirksverwaltungsbehörde) seinem Auskunftsbegehren aus Februar 2012 bisher nicht nachgekommen sei bzw. ihn lediglich telefonisch kontaktiert und um Angabe der näherhin geforderten Daten ersucht habe.

Der Beschwerdeführer begehrte mit einfacher E-Mail aus Februar 2012, ohne Attachment oder elektronische Signatur, vom Beschwerdegegner unter Hinweis auf ein Verwaltungsstraferkenntnis aus Jänner 2012 Auskunft gem § 26 DSG 2000, »ergänzend zu dem Einspruch der im Schreiben angeführten Kennzahl.«

Dieses Auskunftsverlangen wurde von der angeschriebenen Abteilung an die für Datenschutz zuständige Abteilung weitergeleitet. Diese wies die angeschriebene Abteilung an, mit dem

Beschwerdeführer Kontakt aufzunehmen und einen Identitätsnachweis zu verlangen. Ein Mitarbeiter der angeschriebenen Abteilung rief daraufhin den Beschwerdeführer an, erkundigte sich nach dem Umfang der gewünschten Auskunft und wies ihn darauf hin, dass er einen Identitätsnachweis erbringen müsse.

Ein solcher Identitätsnachweis ist nicht erbracht worden, eine schriftliche Antwort auf das Auskunftsbegehren ist nicht ergangen.

Rechtliche Würdigung:
Zunächst war festzuhalten, dass nach der Rechtsprechung der Datenschutzkommission ein Auskunftsbegehren zulässigerweise auch per E-Mail gestellt werden kann (siehe dazu die Bescheide der Datenschutzkommission vom 16. November 2004, GZ K120.959/0009-DSK/2004 und vom 2. Februar 2007, K121.225/0001-DSK/2007 sowie das Erkenntnis des VwGH vom 9. September 2008, Zl 2004/06/0221, wonach auch ein per Fax gestelltes Auskunftsbegehren zulässig ist).

Voraussetzung ist allerdings, dass der Betroffene dem Auftraggeber – wie in § 26 DSG 2000 gefordert – seine Identität nachweist. Durch den Identitätsnachweis soll jedem möglichen Missbrauch des Auskunftsrechts zur Informationsbeschaffung durch Dritte ein Riegel vorgeschoben werden. Ein Auftraggeber darf ohne Vorliegen eines Identitätsnachweises keine Daten an den Auskunftswerber – von dem er in diesem Moment nur annehmen kann, dass er tatsächlich der Betroffene ist – übermitteln, da er sonst das Datengeheimnis gem § 15 Abs. 1 DSG 2000 verletzen könnte (siehe das Erkenntnis des VwGH vom 9. September 2008, Zl 2004/06/0221). Der Identitätsnachweis ist conditio sine qua non für das Entstehen eines inhaltlichen Anspruchs auf Auskunft.

In seinem Erkenntnis vom 9. September 2008, Zl 2004/06/0221, sprach der VwGH aus, dass durch eine eigenhändige Zustellung der begehrten Daten – wie vom Beschwerdeführer in seinem Auskunftsschreiben begehrt – die Erfüllung des Erfordernisses des Identitätsnachweises bei der Stellung des Auskunftsersuchens nicht ersetzt werden kann. Vielmehr hat der Betroffene seine Identität in »geeigneter Form«, dh durch Vorlage eines Identitätsdokumentes in Form einer öffentlichen Urkunde (im Sinne der §§ 292 ff ZPO) im Rahmen seines Auskunftsbegehrens nachzuweisen.

Es kann dem Beschwerdegegner daher im vorliegenden Fall nicht entgegen gehalten werden, wenn er angesichts des Fehlens eines Identitätsnachweises des Beschwerdeführers Zweifel an dessen Identität hegte und diesen insofern innerhalb der in § 26 Abs. 4 DSG 2000 angeordneten Frist von 8 Wochen telefonisch aufforderte, gem § 26 Abs. 1 DSG 2000 seine Identität nachzuweisen, bevor eine inhaltliche Auskunft erteilt werden könne.

Der Beschwerdegegner übersieht dabei aber, dass die Nichterbringung des Identitätsnachweises ihn nicht dazu berechtigt, das Auskunftsverlangen überhaupt ohne schriftliche Antwort zu lassen. Gemäß dem klaren Wortlaut des § 26 Abs. 4 erster Satz DSG 2000 ist in diesem Fall schriftlich zu begründen, warum die Auskunft nicht oder nicht vollständig erteilt werden kann. Aus dem Gesamtzusammenhang des § 26 DSG 2000 ist abzuleiten, dass das Fehlen eines Identitätsnachweises einer der Hinderungsgründe ist, die in einer solchen schriftlichen Antwort an den Auskunftswerber anzuführen sind. Eine bloße vorherige Aufforderung zur Mitwirkung – nämlich eben zur Erbringung des Identitätsnachweises – durch einen Telefonanruf vermag diese schriftliche Ablehnung des Auskunftsbegehrens nicht zu ersetzen.

Der Beschwerde war daher Folge zu geben.

f. Umfang des Auskunftsrechts nach DSG 2000 (K121.954/0006-DSK/2013, 10.4. 2013)

Sachverhalt:

Die Beschwerdeführerin behauptet eine Verletzung im Recht auf Auskunft dadurch, dass die Beschwerdegegnerin (eine Bank) der Aufforderung gem § 26 DSG 2000 zur Mitteilung, welche Produkte für die verpflichtete Partei eines Exekutionsverfahrens, in welchem sie als betreibende Partei fungiere, verwaltet würden, nicht nachgekommen sei.

Die Beschwerdeführerin betreibt ein Exekutionsverfahren gegen die verpflichtete Partei. Mit Beschluss des zuständigen Bezirksgerichtes aus September 2012 wurde die Beschwerdeführerin zur Hereinbringung der vollstreckbaren Forderung samt Zinsen und der Exekutionskosten samt Zinsen zum Zwecke der Verwertung der zufolge des Beschlusses aus Juli 2012 gepfändeten, der verpflichteten Partei zustehenden Vermögensrechte aus Wertpapierdepotkonten bei der Beschwerdegegnerin gem § 333 EO ermächtigt, diese Rechte der verpflichteten Partei in deren Namen geltend zu machen.

Mit Schreiben aus November 2012 forderte die Beschwerdeführerin die Beschwerdegegnerin unter Hinweis auf den Beschluss des Bezirksgerichtes aus September 2012 und unter Hinweis auf das Schreiben der Beschwerdegegnerin aus Oktober 2012 auf, ihr gem § 26 DSG 2000 mitzuteilen, welche Produkte für die verpflichtete Partei verwaltet würden.

Die Beschwerdegegnerin führte dazu aus, ihrer als Drittschuldnerin im Rahmen der Exekutionsordnung bestehenden Pflicht zur Auskunftserteilung mit Drittschuldnererklärungen aus März, Juli und Schreiben aus Oktober 2012 in vollem Umfang nachgekommen zu sein und dass weitere Ersuchen um Auskunftserteilung (in dieser Angelegenheit) nicht mehr beantwortet werden würden.

Rechtliche Würdigung:

Zunächst war zu prüfen, ob die der Beschwerdeführerin erteilte Ermächtigung gem § 333 EO auch das Recht umfasst, im Namen der verpflichteten Partei deren verfassungsrechtlich gewährleistetes, subjektives Recht auf Auskunft gem § 1 Abs. 3 Z 1 in Verbindung mit § 26 DSG 2000 gegenüber der Beschwerdegegnerin geltend zu machen. Dies ist nach Ansicht der Datenschutzkommission nicht der Fall.

Beim Recht auf Auskunft handelt es sich um ein höchstpersönliches, subjektives, verfassungsrechtlich gewährleistetes Recht, welches im Verwaltungsweg vor der Datenschutzkommission durchzusetzen ist und der nachprüfenden Kontrolle der Gerichtshöfe des öffentlichen Rechts unterliegt. So wie alle subjektiven Rechte kann das Recht auf Auskunft grundsätzlich nur vom Betroffenen selbst oder dessen gewillkürten Vertreter im Namen des Betroffenen geltend gemacht werden. Nur wenn der Betroffene selbst noch nicht oder nicht mehr handlungsfähig ist, können dessen (subjektive) Rechte in dessen Namen auch ohne Vorliegen einer gewillkürten Vertretung von einem anderen nach den Bestimmungen des bürgerlichen Rechts geltend gemacht werden.

Durch die zitierten Ermächtigungen der Exekutionsordnung wird der betreibende Gläubiger in die Lage versetzt, im Namen des Verpflichteten (bestimmte) Vermögensrechte geltend zu machen. Die Geltendmachung dieser Rechte hat jedoch auf dem Zivilrechtsweg zu erfolgen (vgl dazu etwa § 333 EO, arg. »nach Maßgabe der Vorschriften des bürgerlichen Rechts«, sowie den Beschluss des OGH vom 30. Mai 1984, GZ 3 Ob 33/84). Die Ermächtigungen der Exekutionsordnung können somit nicht dahin gehend verstanden werden, als ermächtigten sie den Gläubiger, auch höchstpersönliche, subjektive, im Verwaltungsverfahren durchzusetzende Rechte eines Verpflichteten in dessen Namen geltend zu machen. Dies würde dem klaren Wortlaut und dem Sinn der §§ 308 und 333 EO widersprechen.

Die Beschwerdeführerin ist daher nicht als Person anzusehen, der gem § 1 Abs. 3 Z 1 bzw. § 26 Abs. 1 DSG 2000 Auskunft zu erteilen ist. Abgesehen davon, dass die Beschwerdegegnerin auf das Auskunftsersuchen der Beschwerdeführerin reagiert und – mit näherer Begründung – mitgeteilt hat, dass keine (weitere) Auskunft erteilt werde und somit den Erfordernissen des § 26 Abs. 4 DSG 2000, welcher dem Auftraggeber auferlegt, binnen einer Frist von acht Wochen nach Einlangen des Begehrens die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird, entsprochen hat, war die Beschwerde allein schon aus dem Grunde der mangelnden Legitimation zur Stellung des Auskunftsverlangens an die Beschwerdegegnerin abzuweisen.

g. Datenschutzrechtliche Auskunft in englischer Sprache (K121.935/0006-DSK/2013, 22.5. 2013)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass die von der Beschwerdeführerin erteilte datenschutzrechtliche Auskunft inhaltliche Mängel aufweise, (neben anderen Punkten) insb dass Daten auf einem Beiblatt (»Customer Master Data«) auf Englisch beschriftet und »abgeschnitten« seien.

Der Beschwerdeführer ist Kunde der Beschwerdegegnerin und richtete im Februar 2012 ein datenschutzrechtliches Auskunftsbegehren an diese.

Dieses Auskunftsbegehren wurde zunächst (trotz mehrfacher Urgenz) nicht beantwortet, worauf vom Beschwerdeführer das Beschwerdeverfahren eingeleitet wurde. Im Verfahren erteilte die Beschwerdegegnerin dem Beschwerdeführer eine Auskunft, die hinsichtlich des Dateninhalts auf eine Beilage verwies.

Der Auskunft waren zwei Seiten Ausdruck aus einer Datei mit der Bezeichnung »Customer Master Data« (übersetzt etwa: »Kunden-Stammdaten«) angeschlossen. In diesem Ausdruck werden die Bezeichnungen der ausgedruckten Datenarten in englischer Sprache angegeben. Die Dateninhalte sind teils auf Deutsch, teils auf Englisch eingetragen. So ist bei der Datenart »Customer Relation Type« (etwa: Art der Kundenbeziehung) der Inhalt »Hauptkontakt <--> Verbraucher« angegeben, während bei der Datenart »Customer Contact Marital Status« (etwa: »Ehestand der Kontaktperson beim Kunden«) der Inhalt »No Marital Status Assigned« (etwa: »kein Ehestand erfasst«) ausgewiesen wird.

Rechtliche Würdigung:

Hinsichtlich der Behauptung, die teils in englischer Sprache erteilte Auskunft verletze den Beschwerdeführer in seinem Recht auf Auskunft, hat sich die Beschwerde als berechtigt erwiesen.

Gemäß Art. 8 Abs. 1 des B-VG ist die deutsche Sprache, unbeschadet der den sprachlichen Minderheiten bundesgesetzlich eingeräumten Rechte, die Staatssprache der Republik.

Diese Verfassungsbestimmung bindet direkt zwar nur Staatsorgane (ua sind Verfahren vor der Datenschutzkommission zwingend in deutscher Sprache zu führen, vgl das Erkenntnis des VwGH vom 23. 2. 2000, Zl. 2000/12/0026) und hindert Privatpersonen nicht daran, sich auch im Rechtsverkehr (etwa bei der Abfassung von Verträgen) im Konsens anderer Sprachen zu bedienen.

§ 26 Abs. 1 DSG 2000 verpflichtet den datenschutzrechtlich verantwortlichen Auftraggeber aber dazu, Auskünfte »in allgemein verständlicher Form« zu erteilen. Es handelt sich bei der Auskunftserteilung nicht um einen im Konsens erfolgenden Akt der Rechtsgestaltung sondern um die einseitige Erfüllung einer durch Gesetz auferlegten Pflicht. Das Gesetz betont dabei den

Aspekt der Verständlichkeit. In den Datenanwendungen der Beschwerdegegnerin sind die Daten nun, wie festgestellt, zumindest zu einem Großteil unter englischsprachigen Bezeichnungen bzw. mit englischsprachigen Inhalten gespeichert, deren Bedeutung sich für den durchschnittlichen Empfänger nicht erschließt, sodass die Auskunftserteilung zwar nicht als falsch oder unrichtig bezeichnet werden kann, mangels allgemeiner Verständlichkeit aber nicht dem Gesetz entspricht. Da die deutsche Sprache die verfassungsmäßige Amts-, Unterrichts- und allgemeine Verkehrssprache auf dem Staatsgebiet der Republik Österreich ist, den Beschwerdeführer also niemand verpflichten kann, die englische Sprache zu sprechen oder sich ihrer im Rechtsverkehr zu bedienen, hätte die Beschwerdegegnerin englischsprachige Inhalte ihrer Datenanwendungen zumindest durch Beifügung einer entsprechenden Erklärung oder Übersetzung allgemein verständlich machen müssen.

Da sie dies nicht getan hat, hat sie den Beschwerdeführer in seinem Recht auf eine mangelfreie Auskunft verletzt.

h. Auskunftsbegehren durch Rechtsanwalt für einen Mandanten (K121.964/0015-DSK/2013, 6.9. 2013)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass die Beschwerdegegnerin auf sein Auskunftsersuchen vom Jänner 2013 innerhalb der achtwöchigen gesetzlichen Frist nicht reagiert habe.

Die Beschwerdegegnerin forderte den Beschwerdeführer mit Inkassomahnung aus Jänner 2013 zur Zahlung eines bestimmten Betrages auf, da er im Juni 2012 unter Angaben seiner personenbezogenen Daten einen kostenpflichtigen Vertrag auf einer näher genannten Interseite abgeschlossen hatte.

Der vom Beschwerdeführer mandatierte Rechtsanwalt richtete im Jänner 2013 ein Schreiben an die Beschwerdeführerin, welches (hier wesentlich) wie folgt lautet:

»... In einem habe ich Sie aufzufordern, binnen der gesetzlichen Frist mitzuteilen, welche Daten Sie von meinem Mandanten gespeichert haben, an wen Sie diese weitergeleitet haben. ...«

Die Beschwerdegegnerin wies in ihrer Antwort auf den rechtsgültigen Abschluss eines Vertrages hin, nahm jedoch auf das Auskunftsersuchen selbst keinen Bezug.

Rechtliche Würdigung:

§ 26 Abs. 1 DSG 2000 knüpft die Auskunftserteilung an die Bedingung, dass der Betroffene gegenüber dem Auftraggeber seine Identität nachweist. Der Identitätsnachweis ist conditio sine qua non für das Entstehen eines Anspruchs auf inhaltliche Auskunft. Diese Bestimmung hat den klar erkennbaren Zweck, jedem möglichen Missbrauch des Auskunftsrechts zur Informationsbeschaffung durch Dritte einen Riegel vorzuschieben. Ein Auftraggeber darf ohne Vorliegen eines Identitätsnachweises keine Daten an den Auskunftswerber – von dem er in diesem Moment nur annehmen kann, dass er tatsächlich Betroffener ist – übermitteln, da er sonst das Datengeheimnis gemäß § 15 Abs. 1 DSG 2000 verletzen könnte (vgl dazu den Bescheid der Datenschutzkommission vom 4. Mai 2004, GZ K120.905/0008-DSK/2004, sowie auch das Erkenntnis des VwGH vom 9. September 2008, Zl. 2004/06/0221).

Dem Beschwerdeführer war zuzustimmen, dass nach der Rechtsprechung der Datenschutzkommission die Nichterbringung des Identitätsnachweises einen Auftraggeber grundsätzlich nicht dazu berechtigt, das Auskunftsverlangen zur Gänze ohne schriftliche Antwort zu lassen.

Gemäß dem klaren Wortlaut des § 26 Abs. 4 erster Satz DSG 2000 ist in diesem Fall schriftlich zu begründen, warum die Auskunft nicht oder nicht vollständig erteilt werden kann. Aus dem Gesamtzusammenhang des § 26 DSG 2000 ist abzuleiten, dass das Fehlen eines Identitätsnachweises einer der Hinderungsgründe ist, die in einer solchen schriftlichen Antwort an den Auskunftswerber anzuführen sind (vgl dazu etwa zuletzt den Bescheid der Datenschutzkommission vom 10.April 2013, GZ K121.924/0006-DSK/2013).

Der Beschwerdeführer übersieht jedoch, dass an ein von einem rechtskundigen Parteienvertreter verfasstes Auskunftsbegehren strengere Anforderungen zu stellen sind, weil davon auszugehen ist, dass dieser – im Gegensatz zu einem rechtsunkundigen Betroffenen – mit den einschlägigen gesetzlichen Bestimmungen vertraut ist, sodass eine allfällige »Manuduktionspflicht« eines Auftraggebers weitgehend entfällt.

Nach der Rechtsprechung der Datenschutzkommission löst ein an einen rechtsunkundigen Auftraggeber des privaten Bereichs gerichtetes anwaltliches, in der »Ich-Form« verfasstes Schreiben, in welchem lediglich darauf hingewiesen wird, einen Auskunftswerber zu vertreten, ohne dass diesem Schreiben ein Identitätsnachweis des Auskunftswerbers selbst oder eine an den Anwalt vom Auskunftswerber erteilte Vollmacht beigefügt ist, keine Auskunftspflicht eines Auftraggebers aus, weil es sich diesfalls um kein gültiges Auskunftsersuchen im Sinne des § 26 Abs. 1 DSG 2000 handelt. In diesem Fall entfällt auch die Pflicht des Auftraggebers, den Auskunftswerber zur nachträglichen Vorlage eines Identitätsnachweises aufzufordern (vgl dazu den Bescheid der Datenschutzkommission vom 10. Juli 2009, GZ K121.495/0013 DSK/2009).

Da dies auf das vom Rechtsanwalt des Beschwerdeführers verfasste Schreiben vom Jänner 2013 zutrifft, war die Beschwerde sohin mangels Vorliegen eines gültigen Auskunftsersuchens, auf welches die Beschwerdegegnerin hätte reagieren müssen, abzuweisen.

8.1.2 8.1.2 Recht auf Geheimhaltung

a. Telefonische Auskunft zum Stand eines Verfahrens (K121.744/0004-DSK/2012, 24. 2. 2012)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass ein Mitarbeiter des Erstbeschwerdegegners (eine Landesregierung) im Juli 2011 telefonisch bei der Zweitbeschwerdegegnerin (eine Bezirksverwaltungsbehörde) Auskunft über den Stand eines gegen ihn anhängigen Verwaltungsstrafverfahrens erhalten habe.

Die Gesellschaft, für die der Beschwerdeführer als Pilot tätig ist, hat mit Anträgen aus 2011 beim Erstbeschwerdegegner (zuständige Luftfahrtbehörde) um die Erteilung von Bewilligungen gem §§ 9 und 126 des Luftfahrtgesetzes (Bewilligungen für Starts und Landungen außerhalb von Flugplätzen, Genehmigung ziviler Luftfahrtveranstaltungen) angesucht.

Gemäß einem Bericht einer Polizeiinspektion stand der Beschwerdeführer unter Verdacht, im März 2011 als Pilot eines Hubschraubers gegen eine der Auflagen eines Bewilligungsbescheides für Außenlandungen und -abflüge verstoßen zu haben (Nichteinhaltung des Mindestabstands von 100 Metern zu einem Wohngebäude). Bei der Zweitbeschwerdegegnerin war deswegen ein Verwaltungsstrafverfahren wegen des Verdachts von Übertretungen des Luftfahrtgesetzes anhängig.

Im Juli 2011 erkundigte sich ein für das Genehmigungsverfahren nach den §§ 9 und 126 des Luftfahrtgesetzes zuständiger Mitarbeiter des Erstbeschwerdegegners telefonisch bei der Zweitbeschwerdegegnerin nach dem Stand des besagten Verwaltungsstrafverfahrens und

erhielt die Auskunft, es sei eine Verfolgungshandlung gesetzt worden, vom beschuldigten Piloten (dem Beschwerdeführer) fehle aber noch eine Stellungnahme. Dies wurde in einem Aktenvermerk festgehalten.

Rechtliche Würdigung:
Im vorliegenden Beschwerdefall war der Erstbeschwerdegegner nicht abstrakte Oberbehörde, sondern konkret mit Genehmigungsverfahren nach §§ 9 und 126 LFG befasster zuständiger Behördenapparat, für deren Entscheidung die Gesetzestreue und Zuverlässigkeit des Beschwerdeführers in seiner Funktion als Pilot denkmöglich (siehe dazu auch den Bescheid vom 29. November 2005, GZ: K121.046/0016-DSK/2005) von Bedeutung war. Diese Annahme der Denkmöglichkeit gründet sich auf die §§ 9 Abs. 2 und 126 Abs. 2 LFG. Wiederholtes oder nachhaltiges Missachten von Auflagen durch Piloten hätte etwa Anlass zum Widerruf einer Genehmigung für Außenlandungen und -abflüge gem § 9 Abs. 2 letzter Satz LFG geben können.

Der Erstbeschwerdegegner war daher gem § 7 Abs. 1 DSG 2000 iVm § 8 Abs. 4 Z 2 DSG 2000 berechtigt, den Beschwerdeführer betreffende Daten aus dem Verwaltungsstrafverfahren zu ermitteln, die Zweitbeschwerdegegnerin berechtigt, diese gem § 7 Abs. 2 DSG 2000 iVm § 8 Abs. 4 Z 2 DSG 2000 zu übermitteln. Zusätzlich konnten sich die Beschwerdegegner bei ihrem Vorgehen hier auch auf die bundesverfassungsrechtliche Bestimmung über die Leistung von Amtshilfe stützen. Die Beschwerde war daher als unbegründet abzuweisen.

b. Radarüberwachung durch Gemeinde (K121.758/0003-DSK/2012, 24. 2. 2012)

Sachverhalt:
Die Beschwerdeführerin behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass im Auftrag der Beschwerdegegnerin (einer Gemeinde) auf deren Gemeindegebiet eine automatische Geschwindigkeitsüberwachungsanlage (»Radar«) installiert sei, die von einem Privatunternehmen betrieben werde. Im Oktober 2010 sei sie damit als Lenkerin eines Kraftfahrzeuges gemessen und wegen des Verdachts einer Verwaltungsübertretung (nach §§ 52 lit a Z 10a iVm 99 Abs. 3 lit. a StVO) bei der Bezirkshauptmannschaft zur Anzeige gebracht worden. Diese Vorgehensweise sei auch nach neuerer Rechtslage (StVO 1960 in der Fassung der 22. StVO-Novelle, BGBl I 2009/16) unzulässig, da nur die Bezirksverwaltungsbehörde selbst gesetzlich zu solcher Überwachung ermächtigt sei.

Rechtliche Würdigung:
Der Beschwerdegegnerin wurde die Zuständigkeit zur Handhabung der Verkehrspolizei im Gemeindegebiet gem § 94b Abs. 1 lit a und § 94c Abs. 3 StVO 1960 (in Verbindung mit einer Übertragungsverordnung) gesetzmäßig übertragen. Damit obliegt der Beschwerdegegnerin u. a. die Entscheidung, wie die verkehrspolizeiliche Überwachung der Einhaltung der Bestimmungen der StVO 1960 über die zulässige Fahrgeschwindigkeit im Gemeindegebiet organisiert und durchgeführt wird (insb Ort, Zeit und gesetzmäßige Methode der Überwachung).

Die Beschwerdegegnerin handelte daher datenschutzrechtlich im Rahmen ihrer gesetzlichen Zuständigkeiten gem § 7 Abs. 1 DSG 2000. § 98b Abs. 1 und 2 StVO 1960 bildet darüber hinaus eine ausdrückliche gesetzliche Ermächtigung zur Verarbeitung von (personenbezogenen, weil jedenfalls identifizierbaren Betroffenen zuordenbaren) Mess- und Bilddaten (»die zur Identifizierung von Fahrzeugen oder Fahrzeuglenkern geeignet sind«) gem § 8 Abs. 4 Z 1 DSG 2000.

Damit durfte die Beschwerdegegnerin als datenschutzrechtliche Auftraggeberin hier gesetzmäßig in das Recht der Beschwerdeführerin auf Geheimhaltung personenbezogener Daten eingreifen.

Die personenbezogene Verwendung digitaler Bilddaten für Zwecke der Verkehrspolizei und des Verwaltungsstrafverfahrens ist, wie schon oben ausgeführt, von der Ermächtigung gem § 98b Abs. 1 und 2 StVO 1960 umfasst. Die Ansicht der Beschwerdeführerin, die Verwaltungsstraf- bzw. die Verkehrspolizeibehörde müsse »selbst die Fotos machen«, ist jedenfalls für die hier zu beurteilende Frage des Datenschutzrechts unzutreffend:

Gem § 10 Abs. 1 DSG 2000 sind datenschutzrechtliche Auftraggeber nämlich berechtigt, bei ihren Datenanwendungen Dienstleister heranzuziehen. Aus der Heranziehung des Dienstleisters konnte daher keine Verletzung des subjektiven Rechts der Beschwerdeführerin auf Geheimhaltung ihrer Daten resultieren, da eine tatsächliche Verletzung des Datengeheimnisses (§ 15 DSG 2000) durch diesen Dienstleister weder konkret behauptet worden ist, noch sich im Ermittlungsverfahren dafür Anhaltspunkte ergeben haben. Die hier aufgeworfene Frage der grundsätzlichen Entscheidung über die Zulässigkeit des Verwendungsvorgangs (Anordnung der automatischen Überwachung) war Sache des Auftraggebers und nicht des Dienstleisters.

Die Beschwerde war daher spruchgemäß abzuweisen.

c. Weitergabe von Daten betreffend Einwendungen in einem Bauverfahren (K121.763/0003-DSK/2012, 30. 3. 2012)

Sachverhalt:
Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass der Beschwerdegegner (eine Tiroler Bezirksverwaltungsbehörde) in einem Baubewilligungsbescheid zwei seiner Briefe (enthaltend Einwendungen gegen ein Bauvorhaben) »wörtlich veröffentlicht« habe. Dieser Bescheid sei nicht nur an die Parteien des Verfahrens »sondern an über 30 Empfänger gleichsam als Rundschreiben versandt« worden.

Der Beschwerdeführer ist Miteigentümer einer der bauverfahrensgegenständlichen Liegenschaft angrenzenden Liegenschaft. Im Mai 2011 richteten laut Briefkopf mehrere Personen (Nachbarn; darunter aber nicht der Beschwerdeführer) einen Brief an den Bauwerber mit Bedenken hinsichtlich verschiedener Bauangelegenheiten. Das Schreiben enthielt insb Erwägungen zum Inhalt entsprechender vertraglicher Vereinbarungen. Über dem gedruckten Namen des Beschwerdeführers befand sich eine unleserliche eigenhändige Unterschrift. Nur aufgrund der Datenschutzkommission vorliegender, eigenhändig unterschriebener Eingaben des Beschwerdeführers konnte die Feststellung getroffen werden, dass es sich um seine Unterschrift handelt. Auf einem weiteren Brief mit denselben Urhebern, derselben Adressatin und demselben Betreff (mit Beisatz: »Ergänzung unseres Schreibens vom ...«) wurde eigenhändig ausdrücklich mit dem eine Stellvertretung offenlegenden Beisatz »i.V.« unterschrieben, wobei nicht sicher beurteilt werden kann, ob diese Unterschrift vom Beschwerdeführer stammt.

Diese beiden Schreiben wurden im Juli 2011 an den Beschwerdegegner gesendet und in der Niederschrift über die mündliche Bauverhandlung im Juli 2011, an der der Beschwerdeführer nicht teilgenommen hat, bereits in folgender Weise erwähnt:

»Seitens der westlichen Nachbarn wurden bereits vor der mündlichen Verhandlung zwei Schreiben an die Behörde übermittelt. ... Diese beiden Schreiben werden als Parteienerklärungen in den Bescheid aufgenommen. Im Rahmen der mündlichen Verhandlung stimmt der Bewilligungswerber dem Inhalt dieser beiden Schreiben grundsätzlich zu. Eine gesonderte privatrechtliche Vereinbarung wird rechtzeitig vor Baubeginn abgeschlossen werden.«

Mit weiteren Schreiben vom Juli und August 2011 (Ergänzung nach der Bauverhandlung) erhob der Beschwerdeführer begründete Einwendungen gegen das Bauvorhaben. Alle vier

Schreiben sind im Baubewilligungsbescheid vom September 2011 vollständig wiedergegeben. Dieser Bescheid wurde neben der Bauwerberin (und dem planverfassenden Architekten) und acht am Verfahren beteiligten amtlichen Stellen allen zu diesem Zeitpunkt als Parteien nicht präkludierten Nachbarn sowie sieben in der mündlichen Verhandlung im Juli 2011 vertretenen Nachbarn, die keine Einwendungen gegen das Bauvorhaben erhoben hatten, zugestellt (letzteren ohne Zustellnachweis »zur Kenntnis«).

Rechtliche Würdigung:
Diese Beschwerde, die vor dem Hintergrund eines Verfahrens zur Bewilligung eines offenbar vom Beschwerdeführer nachhaltig bekämpften Bauvorhabens zu sehen war, berührte die in der Rechtsprechung vielfach und aus verschiedensten Blickwinkeln behandelte Frage, ob die Verwendung von Angaben, Fakten und Urkundeninhalten, die sich auf bestimmte Personen beziehen, demnach »personenbezogenen Daten« im äußert möglichen Wortsinn der Grundrechtsklausel des § 1 DSG 2000, für Zwecke eines Behördenverfahrens zulässig ist.

Dies wird in stRsp dahin gehend beantwortet, dass sich die Prüfungskompetenz der Datenschutzkommission hier auf Denkmöglichkeits-, insb Zuständigkeitserwägungen und die Wahrung des »Übermaßverbots« beschränkt.

Zuletzt wurde dies für das Arbeitsmarktservice und Ermittlungen für Zwecke eines Verfahrens betreffend Leistungsansprüche aus der Arbeitslosenversicherung wie folgt zusammengefasst (Bescheid der Datenschutzkommission vom 30. September 2011, GZ: K121.722/0008-DSK/2011):

»Was das Vorbringen [der Beschwerdeführerin] angeht, der Beschwerdegegner greife durch ein behördliches Ermittlungsverfahren betreffend Bestehen und Umfang ihrer Leistungsansprüche nach dem AlVG (Notstandshilfe) in ihr Recht auf Geheimhaltung ein, so ist auf die ständige Rechtsprechung der Datenschutzkommission zu verweisen, wonach datenschutzrechtliche Beschwerden nicht geeignet sind, in der Sache vor andere Behörden gehörende Rechtsfragen prüfen zu lassen. Grundsätzlich besteht ein – im Fall eines allgemeinen Verwaltungsverfahrens durch die §§ 37 und 39 Abs. 2 AVG sowie besondere Zuständigkeitsbestimmungen zum Ausdruck kommendes – berechtigtes Interesse der zuständigen Behörde an der Verwendung personenbezogener Daten, insbesondere deren Ermittlung, für Zwecke eines Verwaltungsverfahrens, welches das Interesse der Betroffenen an der Geheimhaltung ihrer personenbezogenen Daten überwiegt, sodass im Allgemeinen schon gemäß §§ 7 Abs. 1 und 8 Abs. 1 Z 4 DSG 2000 eine Verletzung von nach § 1 Abs. 1 leg. cit. bestehenden schutzwürdigen Geheimhaltungsinteressen nicht vorliegt. Als Maßstab für eine Beurteilung der Zulässigkeit der Datenermittlung in solchen Verfahren verbleibt für die Datenschutzkommission das Übermaßverbot als Ausdruck des in § 1 Abs. 2 und § 7 Abs. 3 DSG 2000 normierten Verhältnismäßigkeitsgrundsatzes: Wenn es denkmöglich ist, dass die von einer in der Sache zuständigen Behörde ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet sind, ist die Zulässigkeit der Ermittlung aus datenschutzrechtlicher Sicht gegeben« (vgl u. a. den Bescheid der Datenschutzkommission vom 29. November 2005, GZ: K121.046/0016-DSK/2005).

Hier kam die Datenschutzkommission zu dem Schluss, dass die Wiedergabe von Einwendungen des Beschwerdeführers sowie von Inhalten von Schreiben, die der Beschwerdeführer mit unterzeichnet hat, und die eine privatrechtliche Auseinandersetzung zwischen der Bauwerberin und bestimmten Nachbarn betreffen, im Baubescheid eindeutig verfahrensrelevant und aus datenschutzrechtlicher Sicht daher verhältnismäßig und nicht überschießend war, sowie dass die Zustellung des besagten Bescheids an die Nachbarn gem § 25 Tiroler Bauordnung 2001 ebenfalls verfahrensrelevant und aus datenschutzrechtlicher Sicht daher verhältnismäßig und nicht überschießend war.

Die Fragen, die Inhalte des Bescheids, die gesetzmäßige Verfahrensabwicklung und die mögliche Befangenheit von Verwaltungsorganen betreffen, sind von der zuständigen Berufungsbehörde zu prüfen. Derartige Vorbringen waren für die datenschutzrechtliche Beurteilung durch die Datenschutzkommission nicht von Relevanz.

Offensichtlich unberechtigt war das Vorbringen der Beschwerde dort, wo es geltend macht, die Wiedergabe der Einwendungen des Beschwerdeführers als Partei im betreffenden Verfahren in der Begründung des abschließenden Bescheids stelle einen Eingriff in dessen Recht auf Geheimhaltung dar. Vom Beschwerdeführer wurde dabei nicht dargelegt, wie der Beschwerdegegner als Baubehörde den Pflichten gem §§ 59 und 60 AVG, »alle die Hauptfrage betreffenden Parteienanträge« im Spruch zu erledigen und die entsprechenden Erwägungen rechtlich zu begründen, gesetzmäßig nachkommen sollte, wenn ein entsprechender Antrag weder dargelegt, noch der Name einer Partei genannt werden dürfte. Die Datenschutzkommission hielt daher fest, dass auch durch die vollständige Wiedergabe eines Parteienantrags (inklusiv des Namens der Partei) im Inhalt eines Bescheids das Recht der betreffenden Partei auf Geheimhaltung schutzwürdiger personenbezogener Daten nicht verletzt sein kann.

Die Frage der Zustellung des Bescheids (Zustellverfügung) fällt ebenfalls in den Zuständigkeitsbereich iSd § 7 DSG 2000 der den Bescheid erlassenden Behörde (§ 21 AVG iVm § 5 ZustG), also des Beschwerdegegners. Wie bereits oben ausgeführt, konnte in der Zustellung eines Baubewilligungsbescheids »zur Kenntnisnahme« auch an bereits als Parteien aus dem Verfahren präkludierte Nachbarn kein offenkundig überschießendes Vorgehen des Beschwerdegegners erblickt werden. Der Eintritt der Präklusion gem § 42 Abs. 1 AVG, also des Endes der Parteienstellung, bewirkt für den hier entscheidenden Blickwinkel des datenschutzrechtlichen »berechtigten Interesses« am Verfahren iSd § 8 Abs. 1 DSG 2000 vorrangig den Verlust des Berufungsrechts, nicht jedoch den Verlust jedes Rechts, sich über den Ausgang des Verfahrens zu informieren oder darüber informiert zu werden.

Der Beschwerdeführer wurde daher durch die Vorgehensweise des Beschwerdegegners nicht in seinem Recht auf Geheimhaltung verletzt.

d. Registerzählung (K121.765/0008-DSK/2012, 30. 3. 2012)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass die Beschwerdegegner (an der Registerzählung teilnehmende Behörden) planen würden, zum Stichtag 31. 10. 2011 seine Daten in einem einzigen großen Register zusammenzuführen, um die gemäß dem Registerzählungsgesetz zu diesem Stichtag vorgesehene Volkszählung durchzuführen. Dieses Gesetz widerspreche aber den Vorgaben der EG Verordnung 763/2008, da es die darüber hinausgehende Erfassung einer Vielzahl von Datenarten vorsehe (ua Daten zu Bildungsweg und Bildungsabschlüssen, Präsenz- oder Zivildienst, Erwerbsstatus [erwerbstätig/selbstständig/unselbstständig/Pensionist], Grund einer Erwerbslosigkeit). Es widerspreche weiters dem Grundsatz der Datensparsamkeit und sehe Mittel und Methoden (die Verwendung des bereichsspezifischen Personenkennzeichens für amtliche Statistik – bPK-AS) vor, um zusammengeführte Daten »ohne Verzug« wieder auf eine natürliche Person rückführen zu können (§ 6 Abs. 6 RegzG). Es handle sich daher um personenbezogene Daten gem Art. 2 lit a Richtlinie 95/46/EG und § 4 Z 1 DSG 2000. Die Statistik Austria sei als Empfängerin aller Daten gem § 5 RegzG berechtigt, im Fall von Zweifeln an der Datenqualität diese Rückführung vorzunehmen. Sie verfüge daher über rechtlich zulässige Mittel zur Identifizierung einzelner Betroffener, was den Datenbestand zu unmittelbar personenbezogenen Daten mache. Die Kriterien dafür seien im Gesetz nur unzureichend konkretisiert. Wer Zugang zur Stammzahl einer Person habe, sei in der Lage, daraus das bPK-AS dieser Person zu errechnen. Dies wäre

etwa für die Stammzahlenregisterbehörde (gem E-Gov-G) möglich. Diese Rückführbarkeit widerspreche ebenfalls der EG Verordnung 763/2008, da diese als kleinste statistische Einheit nicht den einzelnen Bürger, sondern die Gemeinde vorsehe. Weiters sehe das RegzG vor, die unter der Sozialversicherungsnummer verarbeiteten Daten der Bildungsdokumentation mit dem bPK-AS zu versehen. Es sei auch zu befürchten, dass die entsprechenden Datenübermittlungen ohne Anwendung einer dem Stand der Technik entsprechenden Verschlüsselungstechnologie erfolgen würden. Die entsprechenden Bestimmungen des RegzG würden gegen das Grundrecht auf Datenschutz (§ 1 Abs. 1 DSG 2000) und das Grundrecht auf Schutz des Privat- und Familienlebens gem Art. 8 Abs. 1 EMRK verstoßen, da zu befürchten sei, dass das Privat- und Familienleben des Beschwerdeführers »ausgespäht« werden solle.

Mit Stichtag im Februar 2012 haben einige Beschwerdegegner der Statistik Austria Verwaltungsdaten übermittelt bzw. hat diese von ihr bereits verarbeitete Daten der Schul- und Hochschulstatistik und des Bildungsstandregisters durch Zweckänderung für Zwecke der Durchführung der gem § 1 Abs. 1 RegzG durchzuführenden Volks-, Arbeitsstätten-, Gebäude- und Wohnungszählung zum Stichtag 31. 10. 2011 verwendet. Es war davon auszugehen, dass sich darunter auch pseudonymisierte (ohne sofortige Feststellbarkeit des Betroffenen verwendete) Daten des Beschwerdeführers im Umfang der Datenarten (Erhebungsmerkmale) laut Anlage zum RegzG befinden, da der Betroffene seinen Hauptwohnsitz in Österreich hat, erwerbstätig ist und Bildungsabschlüsse erworben hat. Mangels eines entsprechenden Erfordernisses wurde eine Identifizierung der Daten des Beschwerdeführers jedoch von der Zweitbeschwerdegegnerin (Statistik Austria) nicht vorgenommen.

Rechtliche Würdigung:
Zur Verfassungsmäßigkeit des RegzG führte die Datenschutzkommission aus, dass sie keine Befugnis habe, die bereits in § 1 Abs. 1 RegzG (samt Festsetzung eines Stichtags) angeordnete Vollziehung jenes Bundesgesetzes zu verbieten, auszusetzen oder durch eine von ihr als Verwaltungsbehörde erster Instanz auszusprechende bescheidmäßige Verfügung nachhaltig, dh über einen gehörig geprüften und erwogenen Einzelfall hinaus, zu behindern. Allein der VfGH erkennt über die Verfassungswidrigkeit von Bundes- und Landesgesetzen (hier: über Individualantrag auf Gesetzesprüfung gem Art. 140 Abs. 1 4. Satz B-VG). Eine Zuständigkeit der Datenschutzkommission in diesem Zusammenhang besteht nicht, sie kann auch kein Gesetzesprüfungsverfahren vor dem VfGH einleiten. Sie müsste vielmehr das RegzG auch dann in verfassungskonformer Auslegung anwenden, wenn sie Bedenken gegen dessen Verfassungsmäßigkeit hätte.

Die Frage, ob eine Volks-, Arbeitsstätten-, Gebäude- und Wohnungszählung gem § 1 Abs. 1 RegzG zum Stichtag 31. 10. 2011 nach der in § 4 RegzG angeordneten Erhebungsart (der Übermittlung und Auswertung pseudonymisierter Verwaltungsdaten) durchzuführen ist, konnte im Sinne des Legalitätsprinzips nur bejaht werden. Dies ist eine klare Entscheidung, eine normative Anordnung des Gesetzgebers an die angesprochenen Verwaltungsorgane, die (unter Drohung individueller Straf- und Disziplinarsanktionen) zu vollziehen ist. Die Möglichkeit für eine verfassungskonforme Interpretation – als Ausdruck der allgemeinen Interpretationsdoktrin, dass erzeugungsmäßig niedrigere Rechtsvorschriften im Hinblick auf die Erzeugungsregeln auszulegen sind – war bei diesen klaren Vorgaben des Gesetzgebers nicht eingeräumt.

Bei Nichtvorliegen von Zweifeln über die Auslegung von Rechtsnormen kommt eine verfassungskonforme Interpretation nicht in Betracht.

Auch der allgemeinen EU-Datenschutzrichtlinie 95/46/EG ist kein Verbot für die Mitgliedstaaten zu entnehmen, gemäß ihren eigenen Rechtsvorschriften Volkszählungen oder andere statistische Erhebungen durchzuführen und dafür auch auf bereits für andere Zwecke verarbei-

tete Verwaltungsdaten zurückzugreifen (Art. 6 Abs. 1 lit. b RL 95/46/EG). Der Erwägungsgrund 29 führt dazu aus: »Die Weiterverarbeitung personenbezogener Daten für historische, statistische oder wissenschaftliche Zwecke ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, wenn der Mitgliedstaat geeignete Garantien vorsieht. Diese Garantien müssen insbesondere ausschließen, daß die Daten für Maßnahmen oder Entscheidungen gegenüber einzelnen Betroffenen verwendet werden.«

Die vom Beschwerdeführer angeführte EU-Volks- und Wohnungszählungsverordnung 2008/763/EG bringt in ihrem Art. 3 klar zum Ausdruck, dass die im Anhang angegebenen Datenarten jedenfalls für Statistikzwecke der Unionsorgane an die Europäische Kommission (Eurostat) zu übermitteln sind. Sie gibt damit einen Mindestrahmen vor. Art. 4 Abs. 1 lit. b VO 2008/763/EG sieht das Mittel der Registerzählung sogar ausdrücklich vor. Erwägungsgrund 8 der zitierten Verordnung spricht von dem Ziel der »Schaffung eines gemeinsamen statistischen Rahmens«, während Art. 4 Abs. 2 VO 2008/763/EG hinsichtlich des Datenschutzes ausdrücklich auf die nationalen Rechtsordnungen verweist. Dieser Rechtsvorschrift des Unionsrechts ist daher kein Gebot zu entnehmen, aus Datenschutzgründen eine über den Umfang der Datenarten laut ihrer Anlage hinausgehende Volkszählung zu unterlassen.

Soweit der Beschwerdeführer vorbrachte, das RegzG missachte die Grundsätze des § 6 Abs. 1 DSG 2000, so war ihm entgegenzuhalten, dass es sich dabei um Grundsätze auf einfachgesetzlicher Ebene handle, die neben dem RegzG stehen. Sie nehmen selbst in mehrfacher Hinsicht (§ 6 Abs. 1 Z 1 und 2 DSG 2000) auf die Rechtmäßigkeit der Datenverwendung Bezug, die auch durch andere Gesetze wie bspw das RegzG bestimmt werden kann. Im Sinne eines interpretatorischen Anwendungsvorrangs ist das RegzG im Verhältnis zu § 6 Abs. 1 DSG 2000 als Spezialnorm anzusehen. Dieses Argument vermag daher keine Gesetzwidrigkeit der Datenverwendung für Zwecke der Registerzählung aufzuzeigen.

Der Beschwerdeführer hat insofern Recht, als es sich bei der Registerzählung um keine Verwendung vollständig anonymisierter oder nur indirekt personenbezogener Daten handle. Es kann nämlich nicht ausgeschlossen werden, dass eine Vielzahl von Datensätzen dem Verfahren nach § 5 Abs. 2 und 5 RegzG unterzogen und zur Abklärung statistischer Qualitätsmängel identifiziert wird. Selbst für die Daten des Beschwerdeführers, der laut Sachverhaltsfeststellungen bisher nicht identifiziert worden ist, kann dies nicht ausgeschlossen werden. Der Gesetzgeber räumt der Statistik Austria jedoch dafür eine rechtliche Befugnis ein bzw. verpflichtet den übermittelnden Auftraggeber (im Sinne der vom DSG 2000 abweichenden Terminologie des RegzG den »Inhaber von Verwaltungsdaten«), bei der Aufhebung der Pseudonymisierung unter Entschlüsselung von bPK und bPK-AS mitzuwirken (allein kann diese von der Statistik Austria mit rechtlich zulässigen Mitteln nicht bewirkt werden). Damit gibt es für die Statistik Austria ein rechtlich zulässiges Mittel zur Herstellung des direkten Personenbezugs, wenn dieses auch auf bestimmte spezielle Anwendungsfälle beschränkt ist. Auch das Vorbringen des Beschwerdeführers, dass allein durch Abgleich der Erhebungsmerkmale Wohnadresse, Geburtsdatum, Geschlecht und Beruf gemäß Anlage zum RegzG eine Identifizierung von vielen Betroffenen möglich wäre, ist plausibel. Bei den Daten der Registerzählung, die von der Statistik Austria verwendet werden, handelt es sich daher um personenbezogene Daten, solange sie mit bPKs verknüpft sind.

Daraus war für den Beschwerdeführer aber insoweit nichts zu gewinnen, als es sich bei der Registerzählung um eine gesetzmäßige Datenverwendung gem § 7 Abs. 1 und 2 und § 8 Abs. 1 Z 1 DSG 2000 iVm § 6 RegzG handelt, die zu einem Eingriff in die schutzwürdigen Geheimhaltungsinteressen der Betroffenen berechtigt. Das System der Pseudonymisierung und der Verwendung von bPKs dient dabei in erster Linie der Stärkung der Geheimhaltung (als

angemessene Garantie gem § 14 Abs. 1 DSG 2000) und vollzieht den Auftrag gem § 46 Abs. 5 DSG 2000 zur »Verschlüsselung« der Betroffenendaten nach.

Die Beschwerde war daher abzuweisen.

e. Veröffentlichung von Beilagen zum Protokoll einer Gemeindevertretungssitzung (K121.766/0003-DSK/2012, 30. 3. 2012)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Löschung dadurch, dass seinem Löschungsbegehren vom Jänner 2011 an den Beschwerdegegner (eine Salzburger Gemeinde) nicht nachgekommen worden sei.

Im November 2010 fand nach Anfrage eines Gemeindevertreters an den Bürgermeister des Beschwerdegegners als 1. Bauinstanz wegen einer Baurechtswidrigkeit auf der ua. im Eigentum des Beschwerdeführers befindlichen Liegenschaft eine baupolizeiliche Überprüfung gem § 15 BauPolG statt, über die eine ua. personenbezogene Daten des Beschwerdeführers enthaltende Verhandlungsschrift aufgesetzt wurde.

Die Beantwortung der Anfrage des Gemeindevertreters an den Bürgermeister war Gegenstand der Sitzung der Gemeindevertretung vom November 2010 und wurde im entsprechenden Sitzungsprotokoll wie folgt festgehalten: »… TOP 12: Berichte des Bürgermeisters … Anfrage vom ... September 2010 betreffend baupolizeiliche Überprüfung betreffend ... Siehe beiliegenden Amtsbericht der Bauamtsleitung vom ... November 2010 …«. In den Beilagen zum Protokoll findet sich ua oben zitierte Verhandlungsschrift sowie der bezogene Amtsbericht.

Protokoll und Beilagen wurden im Zeitraum von November 2010 bis Mai 2011 und dann wieder vom Juli 2011 bis laufend auf der Website des Beschwerdegegners veröffentlicht.

Im Jänner 2011 ersuchte der Beschwerdeführer den Beschwerdegegner per Mail um die Entfernung der Verhandlungsschrift auf der Website. Die Anfrage wurde nie schriftlich beantwortet, lediglich bereits in der Sitzung der Gemeindevertretung vom Dezember 2010 vom Beschwerdegegner mit Verweis auf die Gemeindeordnung mündlich abgelehnt.

Rechtliche Würdigung

Die Datenschutzkommission betonte zunächst, dass die Verwendung von Daten im Zuge einer Gemeindevertretungssitzung und aller damit im Zusammenhang stehenden Akte (wie zB deren Protokollierung) in den Bereich der Hoheitsverwaltung fällt. Konsequenz daraus ist, dass die Verwendung von personenbezogenen Daten gem § 1 Abs. 2 DSG 2000 einer (formal)gesetzlichen Grundlage bedarf.

Dabei ist zu unterscheiden, ob erstens die gegenständliche Verhandlungsschrift vom November 2010 von Gesetzes wegen überhaupt Teil der Niederschrift über die Gemeindevertretungssitzung sein darf und zweitens, ob diese Niederschrift im Internet veröffentlicht, also datenschutzrechtlich übermittelt werden darf.

Zur Aufnahme in das Sitzungsprotokoll wurde erwogen, dass die gegenständliche Verhandlungsschrift Beilage eines Amtsberichtes betreffend eine Anfrage eines Gemeindevertretungsmitglieds an den Bürgermeister war. Die Anfrage, die auch personenbezogene Daten enthalten kann, ist gem § 24 Abs. 2 Salzburger Gemeindeordnung 1994 vom Bürgermeister zu beantworten und Gegenstand einer Gemeindevertretungssitzung (entweder, weil die Beantwortung sofort mündlich erfolgt oder, wenn sie schriftlich erfolgt, über diese Beantwortung in der

darauffolgenden Sitzung der Gemeindevertretung zu berichten ist). Über die Gemeindevertretungssitzung ist gem § 31 Abs. 2 leg cit auch eine Niederschrift aufzunehmen, in welcher der wesentliche Inhalt der Sitzung festzuhalten ist. Für eine Anfragebeantwortung nach § 24 Abs. 2 leg cit ist das jedenfalls der Inhalt der Antwort. Im Konkreten wurde gefragt, was die Baubehörde betreffend einen Bau unternehme. In der Beantwortung wurde darauf hingewiesen, dass durch den Bürgermeister eine baupolizeiliche Überprüfung stattgefunden habe und zum Ergebnis auf das Verhandlungsprotokoll verwiesen. Da diese baupolizeiliche Überprüfung unmittelbare Folge der Anfrage des Gemeindevertretungsmitglieds war, ist die Aufnahme deren Dokumentation in Form der Verhandlungsschrift aus Sicht der Datenschutzkommission zum Inhalt der Antwort gehörig.

Die Aufnahme der Verhandlungsschrift in das Sitzungsprotokoll ist daher durch § 24 Abs. 2 iVm § 31 Abs. 2 Salzburger Gemeindeordnung gesetzlich gedeckt.

Zur Veröffentlichung der Niederschrift im Internet wurde erwogen, dass eine Niederschrift über eine Sitzung der Gemeindevertretung der Nachvollziehbarkeit und Kontrolle der Ereignisse während der Sitzung diene. Dementsprechend bestimmt § 31 Abs. 5 Salzburger Gemeindeordnung 1994, dass einerseits die Mitglieder der Gemeindevertretung in alle Niederschriften, andererseits die Gemeindemitglieder (!) in Niederschriften über öffentliche Sitzungen der Gemeindevertretung beim Gemeindeamt Einsicht nehmen können. Die Sitzungen der Gemeindevertretung sind gem § 28 Abs. 1 leg cit grundsätzlich öffentlich, vom Ausschluss der Öffentlichkeit gem § 28 Abs. 2 leg cit wurde für die konkrete Sitzung der Gemeindevertretung im November 2010 nicht Gebrauch gemacht. Allerdings kann ausgehend vom Sitzungsprotokoll der Gemeindevertretungssitzung auch nicht angenommen werden, dass die hier maßgeblichen Beilagen (Verhandlungsschrift) öffentlich verlesen wurden.

In die Niederschrift der Sitzung der Gemeindevertretung vom November 2010 ist also allen Gemeindemitgliedern im Wege der Auflage beim Gemeindeamt Einsicht zu gewähren. Ein fernelektronischer Zugang ausschließlich für Gemeindemitglieder wäre dementsprechend datenschutzrechtlich unschädlich. Der Zugang durch Veröffentlichung im Internet fand in der genannten Gesetzesbestimmung aber keine Grundlage, weshalb der Beschwerdeführer daher in seinem Recht auf Geheimhaltung personenbezogener Daten (§ 1 DSG 2000) verletzt ist und seinem Löschungsbegehren vom Jänner 2011 daher zu folgen gewesen wäre. Dadurch, dass die Löschung verweigert wurde, wurde der Beschwerdeführer in seinem Recht auf Löschung personenbezogener Daten verletzt.

f. Verwendung von Daten aus dem LMR für Aussendungen eines Bürgermeisters (K121.760/0016-DSK/2012, 25. 4. 2012)

Sachverhalt:

Die Beschwerdeführer behaupten eine Verletzung im Recht auf Geheimhaltung dadurch, dass der Beschwerdegegner (ein Bürgermeister einer steirischen Gemeinde) für Zwecke der Aussendung einerseits zu einer »parteipolitischen Jugendveranstaltung«, andererseits zum »monatlichen Geburtstagskaffee« Daten aus dem Lokalen Melderegister (LMR) verwendet hätte. Dazu existiere weder ein gesetzlicher Auftrag noch ein Gemeinderatsbeschluss.

Tatsächlich ermittelte der Beschwerdegegner vor bzw. im Mai 2011 als Bürgermeister über das seiner Gemeinde zur Verfügung stehende Portal www.kommunalnet.at mittels der Funktion »Geburtstagsliste« die Daten Vor- und Zuname sowie Adresse (ua.) der Beschwerdeführer für Zwecke der Aussendung einerseits von Einladungen zum monatlichen Geburtstagskaffee und andererseits von Einladungen zu einem Jugendtreff, dessen Zweck u. a. auch der Austausch von Ideen und Vorschlägen zur Gestaltung des Angebots für Jugendliche in der Gemeinde war.

Rechtliche Würdigung:
Entgegen der Meinung der Beschwerdeführer war der Beschwerdegegner bei der gegenständlichen Datenverwendung (Ermittlung aus dem LMR sowie Verarbeitung für die Aussendungen) nicht als Privatperson und auch nicht als Mitglied einer politischen Partei tätig. Für sein Handeln als Organ einer Gebietskörperschaft (Bürgermeister) sprach schon der Inhalt der Aussendungen selbst. Wäre die Abfrage des LMR als Privatperson geschehen, wäre die Datenschutzkommission für die Verfolgung einer damit verbundenen Rechtsverletzung auch nicht zuständig (vgl § 5 DSG 2000 iVm § 32 DSG 2000).

Betreffend die Geburtstagseinladungen erwog die Datenschutzkommission, dass der Beschwerdegegner als Organ einer Gebietskörperschaft (Gemeinde) für die Verwendung von personenbezogenen Daten, unabhängig ob automationsunterstützt oder nicht, gem § 1 Abs. Abs. 2 DSG 2000 einer (formal)gesetzlichen Grundlage bedarf. Die Adressdaten für Zwecke der gegenständlichen Verwendung wurden aus dem LMR der Gemeinde ermittelt. Die geforderte gesetzliche Grundlage für diese Ermittlung fehlte aber im gegebenen Zusammenhang, mag auch das Portal www.kommunalnet.at eine Abfrage für den Zweck der Bildung einer Geburtstagsliste (die offenbar der nachfolgenden Gratulation dienen soll) vorsehen.

§ 14 MeldeG trifft keine Aussage darüber, für welche Zwecke das LMR in welcher Weise abrufbar ist. Er regelt lediglich die Führung des Melderegisters. Gem § 20 Abs. 3 letzter Satz MeldeG sind die Bürgermeister zwar ermächtigt, die in ihrem Melderegister enthaltenen oder ihnen gem Abs. 2 übermittelten Meldedaten zu verwenden, sofern diese zur Wahrnehmung der ihnen gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bilden. Dies trifft auf Einladungen zum Geburtstag aber nicht zu. Der Einwand des Beschwerdegegners, mit diesen Veranstaltungen sei auch eine gemeinschaftsfördernde Funktion verbunden, vermochte daran schon deshalb nichts zu ändern, weil ein derartiger Zweck aus dem Wortlaut der Aussendung in keiner Weise ersichtlich ist. § 20 Abs. 3 MeldeG konnte daher nicht angewendet werden.

Gleiches galt für die Bestimmung des § 13 Steiermärkische Gemeindeordnung 1967, die zwar eine gesetzliche Grundlage für Ehrungen durch die Gemeinde vorsieht. Ehrungen können aber gem Abs. 1 leg cit nur Personen betreffen, die sich um die Gemeinde verdient gemacht haben. Einladungen aus Anlass des Geburtstags sind keine Ehrungen im Sinn dieses Gesetzes.

Auch die vom Beschwerdegegner angeführten §§ 177 ff des Steiermärkischen Volksrechtsgesetzes 1986, §§ 3 ff WählerevidenzG, § 27 der Steiermärkischen Landtagswahlordnung (LTWO) und § 29 Abs. 4 der Wiener Gemeindewahlordnung 1996 betreffen andere Fälle als die der gegenständlichen Aussendungen, weshalb aus deren Anführungen für den Beschwerdegegner nichts zu gewinnen war.

Schließlich führte der Beschwerdegegner § 47 DSG 2000 ins Treffen. Diese Bestimmung regelt die Verwendung von Adressdaten für den besonderen Verwendungszweck Benachrichtigung und Befragung von Betroffenen. Die Regelung geht davon aus, dass für diesen Verwendungszweck grundsätzlich die Zustimmung des Betroffenen eingeholt werden muss (vgl Abs. 1). Nur in den Fällen des Abs. 2 kann die Zustimmung entfallen (und muss auch keine Genehmigung der Datenschutzkommission eingeholt werden). Bei einer Gratulation handelt es sich aber entgegen dem Verständnis des Beschwerdegegners nicht um eine Benachrichtigung des Betroffenen, muss dieser doch ein gewisser Informationsgehalt unterstellt werden (die EB zur RV sprechen in diesem Zusammenhang von »berechtigten Informationsinteressen«; wohl aus Sicht des Empfängers gemeint).

Die Datenschutzkommission betonte allerdings auch, dass sie nicht verkennt, dass es sich bei Gratulationen zum Geburtstag durch Gemeindeorgane um ein verbreitetes und oftmals auch beliebtes Phänomen handelt. Mangels gesetzlicher Grundlage, anders als etwa in Niederösterreich mit dem NÖ Ehrungsgesetz oder im Burgenland mit dem Burgenländischen Ehrungsgesetz, musste die Datenschutzkommission der Beschwerde betreffend die Geburtstagsaussendungen stattgeben.

Betreffend die Einladungen zur Jugendveranstaltungen verwies die Datenschutzkommission zu den Erfordernissen einer rechtmäßigen Verwendung auf die obigen Ausführungen, qualifizierte aber anders als Einladungen zum Geburtstag Einladungen zu Informationsveranstaltungen, die die Einbeziehung der Betroffenen in Planungsvorhaben zum Gegenstand haben (hier: Einbeziehung der Jugendlichen in die Planung von Angeboten zur Freizeitgestaltung) als Benachrichtigungen iSd § 47 DSG 2000, sodass die Verwendung von Adressen aus dem LMR für Zwecke dieser Einladungen in § 47 Abs. 2 lit a DSG 2000 eine gesetzliche Grundlage hat, zumal diese Einladung an sämtliche in der Gemeinde wohnhafte Jugendliche versendet wurde. Dadurch ist nämlich sowohl hinsichtlich der Auswahlkriterien für den Betroffenenkreis als auch hinsichtlich des Gegenstands der Benachrichtigung oder Befragung eine Beeinträchtigung der Geheimhaltungsinteressen der Betroffenen nicht zu erkennen. In diesem Punkt war die Beschwerde daher abzuweisen.

g. Zustellungen unter Beigabe des Geburtsdatums (K121.783/0005-DSK/2012, 16. 5. 2012)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass ihm die Beschwerdegegnerin (eine Bezirkshauptmannschaft) im November 2011 eine Strafverfügung postalisch (im Fensterkuvert, weder RSa noch RSb) zustellen habe lassen, wobei seinem Namen, für jeden am Zustellvorgang Beteiligten lesbar, das Geburtsdatum beigefügt worden sei.

Rechtliche Würdigung:

Die Beschwerdegegnerin hat nicht sensible Daten des Beschwerdeführers, nämlich Vorname, Familien-/Nachname, Zustelladresse und Geburtsdatum für Zwecke eines Zustellvorgangs (Adressierung, Ausdruck und Kuvertierung) automationsunterstützt verwendet. Eine ausdrückliche Ermächtigung zur Verwendung des Geburtsdatums für diesen Zweck besteht nicht, sodass erwogen werden musste, ob überwiegende berechtigte Interessen der Beschwerdegegnerin den Eingriff in diesem speziellen Fall gerechtfertigt haben.

Nach langjähriger Spruchpraxis der Datenschutzkommission kann die Beifügung des Geburtsdatums bei Zustellung behördlicher Erledigungen zur Adressierung gerechtfertigt sein. Dies ist dann der Fall, »... wenn aus der fehlerhaften Identifikation des Empfängers besondere Nachteile entstehen könnten, wie etwa dadurch, dass bei Zustellung des amtlichen Schriftstücks an die falsche Person sensible Daten des eigentlichen Adressaten einem Dritten rechtswidrigerweise zur Kenntnis gelangen könnten (K120.794/007-DSK/2002 vom 3. Dezember 2002, ...), bspw. wenn an der Abgabestelle mehrere Personen mit gleichem Namen, aber unterschiedlichen Geburtsdaten leben.

Da der Beschwerdegegner als zustellende Behörde nach den Bestimmungen des Zustellgesetzes zur, Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe' gemäß §§ 21 f AVG verpflichtet war, den Beschwerdeführer als Empfänger möglichst eindeutig zu bezeichnen und nicht in jedem Fall nachprüfen kann, ob konkret an der Abgabestelle namensgleiche Personen wohnhaft sind, verletzte die Verwendung des Geburtsdatums in der Adressierung zwecks eindeutiger Identifikation des Empfängers diesen daher nicht in seinem Recht auf Geheimhaltung personenbezogener Daten, da der vorgenommene Eingriff in sein Geheimhaltungsrecht leichter

wiegt als die Gefahr, die im Fall eines Zustellfehlers seinem Interesse an der Geheimhaltung verwaltungsstrafrechtlicher Vorwürfe gedroht hätte. Strafrechtliche Vorwürfe sind zwar keine sensiblen Daten im Sinne des Gesetzes, durch ihre Einordnung unter die Sonderregel des § 8 Abs. 4 DSG 2000 im Hinblick auf das Geheimhaltungsinteresse jedoch klar ‚sensibler' als das bloße Geburtsdatum.« (Bescheid vom 17. 12. 2010, K121.636/0010-DSK/2010)

Diese Entscheidungen gehen jedoch von einem gesetzmäßigen Zustellvorgang und einer gesetzmäßigen Zustellmethode aus, bei der dem Zustellorgan (dh dem Briefzusteller des beauftragten Postunternehmens) eine Identitätsprüfung aufgetragen war.

Der gesetzmäßig vorgezeichnete Weg für die nachweisliche, physische Zustellung eines Behördendokuments an den genau bezeichneten Empfänger zu eigenen Handen ist im Inland der eigenhändig zuzustellende Rückscheinbrief (RSa-Brief) gem § 21 ZustG iVm Formular 3/1 zur ZustFormV. Eine Verwaltungsstrafverfügung ist gem § 48 Abs. 2 VStG zwingend eigenhändig zuzustellen. Für die Verwaltungsstrafbehörde besteht in diesem Punkt kein Ermessen (etwa aus Zweckmäßigkeits- oder Sparsamkeitserwägungen). Der Gesetzgeber hat diese Anordnung aus dem systematischen Zusammenhang erkennbar getroffen, um sicherzustellen, dass die Strafverfügung den genau zu bezeichnenden Beschuldigten, an den sich der erhöht schutzwürdige Vorwurf einer strafbaren Handlung richtet (vgl § 8 Abs. 4 DSG 2000), auch sicher erreicht, und kein Unbefugter davon Kenntnis erlangt. Mit der eigenhändigen Zustellung erfolgt auch die Identitätsprüfung durch den Zusteller, was einen zusätzlichen Schutz zugunsten der Zustellung an den Empfänger bedeutet.

§ 5 ZustG sieht überdies die eindeutige Bezeichnung des Empfängers vor und schließt für diesen Zweck die Verwendung des Geburtsdatums zur Identifizierung des Empfängers jedenfalls nicht aus. Dies wird auch durch die einschlägigen Erläuterungen zu § 5 ZustG untermauert. Die Bestimmung, dass die Identität des Empfängers möglichst eindeutig zu bezeichnen ist, hat in dieser Form erstmals durch BGBl I 2004/10 in das ZustG Eingang gefunden.

In den EB 22. GP, RV 252 zu § 5 ZustG idF BGBl I 2004/10 ist zu lesen:

»Durch diese Regelung soll die Verantwortung zwischen Behörde und Zustelldienst klar abgegrenzt werden. Die Zustellverfügung ist kein förmlicher Akt und insbesondere kein Bescheid. Auch § 18 Abs. 3 AVG schafft für den Empfänger keinen subjektiven Rechtsanspruch auf die Übermittlung von Mitteilungen der Behörde in einer bestimmten Form; dies gilt sowohl für die Frage, ob überhaupt eine Zustellung erforderlich ist oder etwa eine telefonische Mitteilung genügt, als auch hinsichtlich der unterschiedlichen Arten der Zustellung. … Das Erfordernis einer möglichst eindeutigen Bezeichnung des Empfängers soll eine ausdrücklichere Rechtsgrundlage als bisher dafür schaffen, dass in manchen Fällen das Geburtsdatum als Identifikationsdatum des Empfängers in der Adressierung angeführt wird. Die Datenschutzkommission hat mehrfach entschieden, dass dies dann zulässig ist, wenn nach dem Inhalt des zuzustellenden Schriftstücks (z.B. ein Strafbescheid) die eindeutige Bezeichnung des Empfängers besonders wichtig ist. ...«

Hier erfolgte nun die Zustellung entgegen den eindeutigen Vorgaben des VStG nicht zu eigenen Handen, sondern durch bloße Abgabe in den Hausbriefkasten. Durch eine Zustellung zu eigenen Handen wäre durch den Zusteller sicher gestellt gewesen wäre, dass nur der Empfänger der Sendung von dem Umstand Kenntnis erlangt hätte, dass gegen ihn eine Strafverfügung erlassen worden ist. Wäre doch durch die Angabe des Geburtsdatums bei korrekter Vorgangsweise der Zusteller in der Lage gewesen, die Sendung dem richtigen Empfänger zuzuordnen und für eine persönliche Aushändigung zu sorgen. Bei der hier erfolgten Zustellung durch bloße Abgabe in den Hausbriefkasten ermöglichte die Angabe des Geburtsdatums zwar auch im Fall na-

mensgleicher Personen im selben Haushalt die richtige Zuordnung unter den Mitbewohnern, verhinderte aber nicht die mögliche Kenntnis eines Mitbewohners über die Tatsache, dass ein behördliches Schriftstück (Strafverfügung) an einen anderen Mitbewohner zugestellt wurde. Da die gesetzlich vorgesehenen strengeren Auflagen für die Zustellung einer Strafverfügung auch den Geheimhaltungsinteressen des Beschwerdeführers dienen, kann sich die Beschwerdegegnerin, die diese gesetzlichen Vorgaben nicht eingehalten hat, nicht auf überwiegende berechtigte Interessen berufen und wurde auch dem datenschutzrechtlichen Verhältnismäßigkeitsgebot nicht entsprochen (§ 1 Abs. 2 DSG).

Der Beschwerde war daher hier Folge zu geben und eine Verletzung des Rechts auf Geheimhaltung festzustellen.

h. Umfrage unter AMS-Kunden (K121.807/0009-DSK/2012, 13. 7. 2012)

Sachverhalt:

Die Beschwerdeführerin behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass der Beschwerdegegner (eine Landesgeschäftsstelle des Arbeitsmarktservices (AMS)), entgegen ihrem Widerspruch (sie sei nicht beim Beschwerdegegner gemeldet), weiterhin sie betreffende Daten verwende und diese dazu benutzt habe, der B Gesellschaft die Durchführung einer im Jänner 2012 per E-Mail angekündigten telefonischen Umfrage unter AMS-Kundinnen und -Kunden zu ermöglichen.

Das AMS verarbeitet automationsunterstützt Daten der Beschwerdeführerin, darunter ihren Namen, ihre Telefonnummer und ihre E-Mail-Adresse. Die Beschwerdeführerin hat sich zuletzt als Arbeitsuchende mit einem Antrag auf Gewährung von Leistungen der Arbeitslosenversicherung im September 2011 an die betreffende Regionalgeschäftsstelle des AMS gewandt. Außerdem war sie als potenzielle Arbeitgeberin beim AMS registriert. Jedenfalls im Oktober 2010 hat sie gegenüber der Regionalgeschäftsstelle jeder »Weitergabe« ihrer Daten ohne ausdrückliche Zustimmung schriftlich widersprochen.

Im Jänner 2012 richtete die B Gesellschaft, ein von der Bundesgeschäftsstelle des AMS beauftragtes Markt- und Meinungsforschungsinstitut, eine E-Mail an die Adresse der Beschwerdeführerin. Darin wurde die – direkt namentlich angesprochene – Beschwerdeführerin unter einem Briefkopf mit den Logos des AMS und der B Gesellschaft um ihre Mitwirkung bei einer telefonischen Befragung zur Zufriedenheit der AMS-Kunden ersucht und ein möglicher Telefonkontakt (Auswahl nach dem Zufallsprinzip) für diesen Zweck angekündigt.

Rechtliche Würdigung:

Zunächst ergab eine Wertung des Sachverhalts klar, dass hier keine Übermittlung von Daten der Beschwerdeführerin, sondern vielmehr eine Überlassung dieser Daten gem § 4 Z 4, 5 und 11 DSG 2000 zwischen dem AMS als datenschutzrechtlich verantwortlichem Auftraggeber und der B Gesellschaft als Dienstleisterin vorliegt. Gesetzliche Bestimmungen, die sich nur auf die Übermittlung von Daten beziehen, wie § 7 Abs. 2 DSG 2000, sind daher auf den Beschwerdefall nicht anzuwenden.

Für die Verwendung der Daten Name, Telefonnummer und E-Mail-Adresse der Beschwerdeführerin (sowohl als Partei eines Verfahrens nach dem AlVG als auch als Kundin des AMS in der Rolle als potenzieller Arbeitgeberin) bestehen ausdrückliche Ermächtigungen in § 25 Abs. 1 Z 1 lit. a), f) und g) sowie Z 6 lit. a), b), k) und l) AMSG.

Die Durchführung einer Studie über die Zufriedenheit der vom AMS betreuten Verfahrensparteien und Kunden fällt unter die gesetzlichen Aufgaben gem § 30 Abs. 1 und 2 AMSG,

die Heranziehung einer externen Einrichtung dazu ist in § 30 Abs. 3 AMSG vom Gesetz ausdrücklich vorgesehen. Die Datenüberlassung für eine entsprechende Forschungsarbeit kann sich wiederum auf die ausdrückliche Ermächtigung gem § 25 Abs. 4 und 5 AMSG stützen.

Was den von der Beschwerdeführerin geltend gemachten, nachweislich erhobenen Widerspruch gegen jede Weitergabe von Daten (Übermittlung als auch Überlassung) betrifft, so liegt im vorliegenden Fall eine gem § 28 Abs. 1 1. Satz DSG 2000 gesetzlich vorgesehene Verwendung von Daten vor. Es konnte von der Antragstellerin kein sich aus ihrer besonderen Situation ergebendes Interesse an der Geheimhaltung der verarbeiteten Daten dargelegt werden, das bei einer Durchschnittsbetrachtung bei anderen Betroffenen nicht vorliegt. Die Datenverwendung entsprach damit den §§ 7 Abs. 1 und 8 Abs. 1 Z 1 DSG 2000, weshalb die Beschwerde als inhaltlich unbegründet abzuweisen war.

i. Verdeckte Ermittlung (K121.812/0006-DSK/2012, 13. 7. 2012)

Sachverhalt:

Der Beschwerdeführer wandte sich zunächst mit einer Beschwerde nach § 88 Abs. 2 SPG im November 2010 an den Unabhängigen Verwaltungssenat Wien (UVS Wien). Darin behauptete er eine Verletzung im Recht auf gesetzmäßiges Handeln der Sicherheitsbehörden dadurch, dass der Beschwerdeführer Zielperson eines sicherheits- bzw. kriminalpolizeilichen Ermittlungsverfahrens des Beschwerdegegners (Bundesministerium für Inneres, Bundeskriminalamt) geworden sei, das im März 2010 zu einer Anklage gegen den Beschwerdeführer (ua wegen Mitgliedschaft in einer kriminellen Organisation) und andere vor einem Landesgericht geführt habe. Für diesen Zweck hätte der Beschwerdegegner – rechtswidrig – im April 2007 eine verdeckte Ermittlerin (VE) in den Verein, in welchem der Beschwerdeführer tätig war, eingeschleust, die sich bis zu ihrem Abzug im Juli 2008 an den politischen Vereinsaktivitäten beteiligt und darüber laufend Bericht erstattet hätte. Erst im November 2010 habe der Beschwerdeführer in der Hauptverhandlung vor dem Landesgericht von diesen Fakten Kenntnis erlangt. Er erhob deswegen Beschwerde an den UVS Wien.

Der UVS Wien leitete die Beschwerde – ohne bscheidförmigen Abspruch – im Jänner 2012 gem § 6 Abs. 1 AVG an die Datenschutzkommission weiter. Im Begleitschreiben wird dazu ausgeführt, man stütze sich auf eine entsprechende Anregung des Beschwerdegegners, wonach hier § 90 SPG 2000 anzuwenden wäre, da »das verdeckte Eindringen in die Privatsphäre« und das Ermitteln personenbezogener Daten »geradezu ein Charakteristikum verdeckter Ermittlungen« darstelle. Im Übrigen sei das in Beschwerde gezogene Verfahren kriminalpolizeilicher Natur gewesen und habe sich »nur zum Schein auf das SPG gestützt«, da die StPO damals noch keine entsprechenden Ermittlungsschritte vorgesehen habe. Eine Datenermittlung durch Anwendung oder Androhung von Befehls- oder Zwangsgewalt sei nicht einmal behauptet worden.

Rechtliche Würdigung:

Da rein faktisch inzwischen jedes behördliche Ermittlungsverfahren mit der regelmäßig automationsunterstützten Verwendung personenbezogener Daten verbunden ist, wies die Datenschutzkommission zunächst darauf hin, dass auf die speziellen rechtlichen Charakteristika der in Beschwerde gezogenen Handlungen und der als verletzt bezeichneten Rechte abgestellt werden muss, um zu sinnvollen und sachgerechten Zuständigkeitsabgrenzungen zu gelangen. Andernfalls würde man regelmäßig zu einer Beinahe-Allzuständigkeit der Datenschutzkommission gelangen, die gleichzeitig, wie vom Beschwerdeführer zutreffend angemerkt, mit einer Entwertung anderer Rechtsschutzverfahren, wie des Beschwerderechts nach § 88 Abs. 2 SPG, Hand in Hand gehen müsste. Aus der Tatsache allein, dass in einem Behördenverfahren personenbezogene Daten verwendet worden sind, kann daher noch keine Zuständigkeit der Datenschutzkommission abgeleitet werden.

Seit Inkrafttreten der DSG-Novelle 2010 ist überdies zu beachten, dass datenschutzrechtlich relevante Handlungen, die ein Staatsorgan »im Dienste der Gerichtsbarkeit« vornimmt, nicht mehr der Kognition der Datenschutzkommission unterliegen (funktionaler Organbegriff, vgl RV, 472 BlgNR 24. GP 13). Dies trifft insb auf die gesamte »Datensammlung« zu, die Organe der Kriminalpolizei für Zwecke einer späteren strafrechtlichen Anklage über das Handeln natürlicher oder juristischer Personen vornehmen (das kriminalpolizeiliche Ermittlungsverfahren gem 2. Hauptstück der StPO in der seit 1. Jänner 2008 gem BGBl I 2004/19 anzuwendenden Fassung). Es handelt sich, so § 18 Abs. 1 SPG, um Tätigkeiten und »Aufgaben im Dienste der Strafrechtspflege (Art. 10 Abs. 1 Z 6 B-VG)«. Da die Staatsanwälte und mit ihnen auch die Staatsanwaltschaften gem Art. 90a B-VG zu den Organen der Gerichtsbarkeit zählen, ist auch kriminalpolizeiliche Arbeit im Ermittlungsverfahren unter Leitungs- und Weisungsbefugnis der Staatsanwaltschaft und des zuständigen Gerichts (§§ 20 Abs. 1 und 99 Abs. 1 StPO) eine Tätigkeit »im Dienste der Gerichtsbarkeit«. Schon der im Beschwerdefall zeitlich bereits im ersten Teil der Tätigkeit der VE (bis Jänner 2008) anwendbare § 22 Abs. 3 SPG legte fest, dass Ermittlungen gegen bestimmte, einer Straftat für verdächtig erachtete Personen, nach den Bestimmungen der StPO zu führen sind, demnach nicht zur eigentlichen Sicherheitsverwaltung zählen.

Die Datenermittlung betreffend bestimmte Verdächtige für Zwecke kriminalpolizeilicher Ermittlungsverfahren kann daher zwar grundsätzlich gem § 31 Abs. 2 DSG 2000 nicht vor der Datenschutzkommission angefochten werden (seit 1. Jänner 2008 war hier jedoch gem § 106 Abs. 1 iVm § 514 Abs. 1 StPO wegen Verletzung subjektiver Rechte im Ermittlungsverfahren der Rechtsbehelf des Einspruchs beim zuständigen Strafgericht möglich, allerdings nur insoweit, als eine Ermittlungsmaßnahme unter Verletzung der StPO angeordnet oder durchgeführt wurde und nach § 107 StPO das Ermittlungsverfahren noch nicht abgeschlossen worden ist).

Die vom VfGH in VfSlg 19.281/2010 vorgenommene Auslegung von § 106 Abs. 1 StPO betrifft die Abgrenzung der Zuständigkeit der UVS von jener der Gerichte und nicht die Zuständigkeit der Datenschutzkommission, die nach § 31 Abs. 2 DSG 2000 zu beurteilen ist. Aus dem Erkenntnis ergibt sich, dass Beschwerden über polizeiliches Handeln im Dienste der Strafjustiz, das die Sicherheitsbehörde »aus eigener Macht« setzt (Fehlen oder Überschreiten einer staatsanwaltschaftlichen Anordnung), aufgrund des verfassungsrechtlichen Grundsatzes der Gewaltentrennung nicht in die Zuständigkeit der Gerichtsbarkeit fallen.

Im vorliegenden Fall war der Einsatz der VE nicht durch eine entsprechende Anordnung der Staatsanwaltschaft gedeckt. Der Beschwerdegegner rechtfertigt seine Vorgangsweise jedenfalls nicht mit der Behauptung, einem Auftrag der Staatsanwaltschaft entsprochen zu haben, sondern verweist lediglich auf die kriminalpolizeiliche Natur des Verfahrens. Vor diesem Hintergrund sind die vom Beschwerdeführer beanstandeten Aktivitäten der VE grundsätzlich als der Exekutive zurechenbare Verwaltungsakte iSd Art. 20 Abs. 1 B-VG anzusehen.

Schon aus der Natur eines verdeckten Einsatzes, aber auch aus dem Parteienvorbringen ergibt sich, dass dabei keine Befehls- und Zwangsgewalt ausgeübt worden ist. Entsprechend § 88 Abs. 2 SPG sind die UVS auch für Beschwerden von Personen zuständig, die behaupten, »auf andere Weise« – als durch Befehls- und Zwangsgewalt – durch »die Besorgung der Sicherheitsverwaltung in ihren Rechten verletzt worden zu sein...«. Im Vergleich zu diesem allgemeinen Auffangtatbestand sind die Voraussetzungen für die Zuständigkeit der Datenschutzkommission nach § 90 SPG spezifischer und könnten abhängig von den Umständen des Falls als lex specialis angesehen werden. Demnach entscheidet die Datenschutzkommission gem § 31 DSG 2000 über Beschwerden wegen einer Rechtsverletzung durch Verwenden personenbezogener Daten in Angelegenheiten der Sicherheitsverwaltung entgegen den Bestimmungen des Datenschutzgesetzes.

Der Beschwerdeführer ließ allerdings im Hinblick auf die Weiterleitung seiner Beschwerde vom UVS Wien an die Datenschutzkommission keinerlei Zweifel daran, dass Beschwerdekern gerade nicht ein datenschutzrechtliches Begehren ist. Er rügt vielmehr ausdrücklich einen Eingriff in sein subjektives Recht auf Gesetzmäßigkeit der Sicherheitsverwaltung gem § 87 iVm § 88 Abs. 2 SPG, welches Recht jedenfalls nicht vor der Datenschutzkommission geltend gemacht werden kann (ob der ursprünglich angerufene UVS Wien im Lichte des oben gesagten zuständig wäre, konnte für die Datenschutzkommission dahingestellt bleiben). Überhaupt sieht der Beschwerdeführer offenkundig weniger sein Recht auf Geheimhaltung von Daten als vielmehr aufgrund des »durch Täuschung hergestellten persönlichen Kontaktes« und der »Einschleichung in die Wohnung« sein Privatleben, seine Eigentumsrechte sowie Ansprüche nach § 87 SPG auf sicherheitspolizeiliche Maßnahmen nur im gesetzlich zulässigen Umfang durch Handlungen des Beschwerdegegners als verletzt.

Für die Geltendmachung all dieser Rechte besteht keine Zuständigkeit der Datenschutzkommission.

Entsprechend der zuvor beschriebenen Ansichten wurde die Beschwerde auch auf § 88 SPG gestützt zunächst an den UVS Wien gerichtet und erst in der Folge an die Datenschutzkommission weitergeleitet. Begehren und Begründung des Beschwerdeführers konzentrieren sich durchwegs auf andere als datenschutzrechtliche Aspekte. Der Beschwerdeführer moniert auch in seinem ergänzenden Vorbringen, dass sich die ursprünglich eingebrachte Beschwerde nicht gegen die von der verdeckten Ermittlerin ausgehende Datenermittlung richtet, sondern gegen die aus seiner Sicht SPG- und StPO-widrige Ermittlungsmethode. Für diese Rechtmäßigkeitsbeurteilung erachtet er den UVS für zuständig. Wie eingangs ausgeführt, muss bei der Abgrenzung von § 88 Abs. 2 und § 90 SPG auf die beanstandeten Handlungen und die als verletzt erachteten Rechte abgestellt werden. Beides begründet im vorliegenden Fall nicht die Zuständigkeit der Datenschutzkommission.

Aus diesen Erwägungen war die Beschwerde daher zurückzuweisen.

j. Telefonische Datenübermittlung durch AMS (K121.817/0016-DSK/2012, 3. 8. 2012)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass eine Landesgeschäftsstelle des Arbeitsmarktservice (AMS) im Jänner 2012 in einem oder mehreren Anrufen ihn betreffende personenbezogene Daten an einen (namentlich bekannten) Dritten, mit dem er seit einiger Zeit im Streit liege, übermittelt habe. Jener habe diese Daten in weiterer Folge zusammen mit höhnischen Kommentaren sofort auf einer Blogsite veröffentlicht, um seinem Ansehen zu schaden. Der Beschwerdeführer beantragte auch, dem Beschwerdegegner derartige Auskünfte für die Zukunft zu untersagen.

Tatsächlich rief ein nicht identifizierter Dritter im Jänner 2012 mehrfach bei der telefonisch erreichbaren »ServiceLine« der AMS-Landesgeschäftsstelle an. Der Unbekannte gab sich als der Beschwerdeführer aus, nannte dessen Sozialversicherungsnummer (SVNr) und erhielt jedenfalls folgende Daten des Beschwerdeführers übermittelt: die Adresse (Meldeadresse des Hauptwohnsitzes), die Höhe des Leistungsbezuges, die zuständige Regionalgeschäftsstelle sowie Kalenderdatum und Zeit des nächsten Kontrolltermins dort, die Dauer des Leistungsbezugs und die Bankverbindung (Bankleitzahl und Kontonummer). In der Folge wurden diese Daten auch im näher bezeichneten Blog veröffentlicht.

Rechtliche Würdigung:
Die Beschwerde hat sich in der Sache als berechtigt erwiesen.

Dem Beschwerdeführer war dabei beizupflichten, wenn er ausführt, dass der Beschwerdegegner durch die Praxis, Auskünfte zu konkreten Verfahren auch telefonisch gegen bloße Nennung der SVNr zu erteilen, entgegen §§ 6 Abs. 1 und 14 Abs. 1 DSG 2000 handelt.

Der Bezug des Beschwerdegegners auf das Recht auf Auskunft nach § 26 Abs. 1 DSG 2000 war deshalb verfehlt, weil der Gesetzgeber die Ausübung dieses Rechts an strenge Kautelen, nämlich ein grundsätzlich schriftlich zu stellendes Auskunftsverlangen samt Erbringung eines Identitätsnachweises, knüpft. Der VwGH fordert in seiner Rechtsprechung für einen solchen Identitätsnachweis einen »hohen Grad an Verlässlichkeit« (VwGH 9. 9. 2008, 2004/06/0221).

Die Nennung der SVNr ist jedenfalls nicht geeignet, die Identität eines Anrufers mit der versicherten Person mit der gebotenen Verlässlichkeit nachzuweisen. Sie wird im Geschäfts- und Behördenverkehr häufig als Identifikator verwendet. Sie muss beim Eintritt in ein Dienstverhältnis dem Arbeitgeber (zwecks Anmeldung des Dienstverhältnisses beim zuständigen Sozialversicherungsträger) ebenso bekannt gegeben werden wie (durch Vorweisung der Sozialversicherungskarte oder »E-Card«) bei jeder Konsultation eines Kassenarztes. Sie scheint auf häufig gebrauchten sozialversicherungsrechtlichen Urkunden wie Krankenstandbestätigungen, ärztlichen Verordnungen und Kassenrezepten in vielfacher Zahl auf und dient (ua in Verfahren des Beschwerdegegners) als Personenkennzahl und Ordnungsbegriff, wird daher in Datenanwendungen einer Vielzahl von Behörden und Betrieben (wie Spitälern, Arztpraxen und Apotheken) verarbeitet. Zwar sind die jeweiligen datenschutzrechtlichen Auftraggeber an das Datengeheimnis gebunden, doch muss allein aus dem hohen Verbreitungsgrad des Datums der zwingende Schluss gezogen werden, dass es als telefonischer Identitätsnachweis faktisch ungeeignet ist.

Es wird aber nicht übersehen, dass dem Beschwerdegegner bei seinen gesetzlichen Aufgaben ein schwieriger Balanceakt zwischen Datenschutz und Kunden- bzw. Parteienfreundlichkeit aufgetragen ist. § 25 AMSG schweigt zu dieser Frage, schließt aber eine Datenübermittlung an unbeteiligte Dritte ebenso aus wie die allgemeine Vorschrift des § 7 Abs. 2 DSG 2000. In Ermangelung einer speziellen gesetzlichen Regelung, die überdies die verfassungsrechtlichen Grenzen des § 1 Abs. 2 DSG 2000 zu beachten hätte, muss jedoch der Schluss gezogen werden, dass die hier aufgezeigte Praxis der telefonischen Datenübermittlung unzulässig ist.

Im Beschwerdefall hat dies dazu geführt, dass Daten des Beschwerdeführers zu dessen Nachteil entgegen § 7 Abs. 2 Z 2 DSG 2000 einem nicht-legitimierten Empfänger, der vor einer vergleichsweise simplen Täuschungshandlung (telefonische Nennung eines fremden Namens und einer fremden Sozialversicherungsnummer) nicht zurückschreckte, übermittelt wurden. Dadurch wurde der Beschwerdeführer in seinem Recht auf Geheimhaltung verletzt.

Der Beschwerdegegner wurde iSd § 14 Abs. 1 DSG 2000 darauf hingewiesen, unverzüglich organisatorische und technische Vorkehrungen zu treffen, die eine Wiederholung derartiger Vorfälle ausschließen (etwa die Vergabe einer nur der Partei des AMS-Verfahrens bekanntzugebenden verfahrens- oder transaktionsbezogenen Geheimzahl, die bei telefonischen Auskunftsbegehren nachweislich zu nennen ist, ähnlich der Praxis im telefonischen Geschäftsverkehr von Banken).

Soweit der Beschwerdeführer die Erlassung eines entsprechenden Auftrags begehrt hat, war sein Anbringen jedoch aufgrund von § 31 Abs. 7 DSG 2000 in Verbindung mit § 40 Abs. 4 DSG 2000 als unzulässig zurückzuweisen.

k. Datenermittlung in Jugendwohlfahrtsangelegenheiten (K121.827/0008-DSK/2012, 14. 9. 2012)

Sachverhalt:

Die Beschwerdeführerin behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass die Beschwerdegegnerin (eine Bezirkshauptmannschaft) im Februar 2012 durch E-Mail-Wechsel zwischen Mitarbeitern der Abteilungen für Jugendwohlfahrt und Verwaltungsstrafrecht die Beschwerdeführerin betreffende Daten (nämlich zu sämtlichen eingetragenen, offenen Strafen, die über sie verhängt worden seien) für ein Verfahren betreffend Obsorge (für ihren Enkel), die ihrer Tochter entzogen werden solle, ermittelt bzw. übermittelt habe.

Die Beschwerdegegnerin führt im Rahmen ihrer gesetzlichen Aufgaben als Jugendwohlfahrtsbehörde ein Verfahren betreffend die Frage, ob die Obsorge für den minderjährigen A der B, der Tochter der Beschwerdeführerin, entzogen werden soll, um Maßnahmen der behördlichen Erziehungshilfe auch gegen den Willen der Mutter zu gewährleisten. Dieses Verfahren war im Februar 2012 gerichtsanhängig.

Im Februar 2012 richtete eine Mitarbeiterin der Abteilung für Jugendwohlfahrt folgende (wesentliche) E-Mail an einen Mitarbeiter von der für Strafen und Vollstreckungsmaßnahmen zuständigen Abteilung der Beschwerdegegnerin: »... Wie Sie wissen, sind wir derzeit mit der Sache A intensiv befasst. Die mütterliche Großmutter [Beschwerdeführerin] führt immer wieder ins Treffen, die Unterbringung des Kindes hätte ausschließlich damit zu tun gehabt, dass eine Verkehrsstrafe nicht bezahlt war. Um für die kommende Tagsatzung vorbereitet zu sein ersuche ich Sie, unserer Aufgabengruppe mitzuteilen, ob gegen [sie] noch weitere Strafverfahren oder deren Bezahlung offen sind, die dazu führen könnten, dass wieder eine Ersatzfreiheitsstrafe in Betracht gezogen werden muss. ...«

In der Antwort vom Februar 2012 wurde die offenen Strafen der Beschwerdeführerin (Aktenzeichen, betreibende Behörde, Betrag) mitgeteilt.

Rechtliche Würdigung:

Die Beschwerde hat sich als nicht berechtigt erwiesen.

Gegenstand war eine Übermittlung von Daten durch behördeninterne Zweckänderung (innerbehördliche Quasi-Amtshilfe, »Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers«) gem § 4 Z 12 letzter Halbsatz DSG 2000.

Der oberösterreichische Landesgesetzgeber hat in § 5c Abs. 4 Z 2 Oö. JWG 1991 an die Bezirksverwaltungsbehörden als Jugendwohlfahrtsbehörden eine auf den Beschwerdefall anwendbare Ermächtigung zur Datenermittlung erteilt. Diese umfasst die Erlaubnis, betreffend bestimmte Bezugspersonen von unter Aufsicht der Jugendwohlfahrtsbehörde stehenden Minderjährigen »Daten, die zur Beurteilung des Kindeswohls oder zur Ermittlung des Kindeswillens erforderlich sind« für den Zweck von Stellungnahmen vor dem zur Entscheidung zuständigen Gericht zu verwenden (also u. a. zu ermitteln, vgl § 4 Z 8 DSG 2000).

Die Beschwerdegegnerin hatte in ausreichender Weise dargelegt, dass die verwendeten Daten denkmöglich für diesen Zweck benötigt wurden. Die Verwendung des Begriffes »Beurteilung« indiziert überdies, dass der Gesetzgeber den Jugendwohlfahrtsbehörden hier einen gewissen Spielraum gestatten wollte, um im Interesse des Minderjährigen Ermittlungen anzustellen und Argumente zu sammeln, über deren Stichhaltigkeit zu entscheiden Sache des zuständigen Gerichts ist.

Dabei ist zu betonen, dass die Beschwerdegegnerin im Rahmen ihrer Aufgaben als Organ des Jugendwohlfahrtsträgers und damit in Verfolgung eines gesetzmäßigen Zwecks tätig geworden ist. Dazu ist auf die Rechtsprechung zur Denkmöglichkeit behördlicher Ermittlungsschritte zu verweisen:

»Datenschutzrechtliche Beschwerden sind nicht geeignet, in der Sache vor andere Behörden gehörende Rechtsfragen ... prüfen zu lassen. Grundsätzlich besteht ein – im Fall von Verwaltungsübertretungen insbesondere durch § 25 Abs. 1 iVm § 26 Abs. 1 VStG, im allgemeinen Verwaltungsverfahren durch die §§ 37 und 39 Abs. 2 AVG sowie besondere Zuständigkeitsbestimmungen zum Ausdruck kommendes – berechtigtes Interesse der zuständigen Behörde an der Verwendung personenbezogener Daten, insbesondere deren Ermittlung, für Zwecke eines Verwaltungs(straf)verfahrens, welches das Interesse der Betroffenen an der Geheimhaltung ihrer personenbezogenen Daten überwiegt, sodass gemäß § 8 Abs. 1 Z 4 bzw. § 8 Abs. 4 Z 3 DSG 2000 eine Veletzung von nach § 1 Abs. 1 leg. cit. bestehenden schutzwürdigen Geheimhaltungsinteressen nicht vorliegt. Als Maßstab für eine Beurteilung der Zulässigkeit der Datenermittlung in solchen Verfahren verbleibt für die Datenschutzkommission das Übermaßverbot als Ausdruck des in § 1 Abs. 2 und § 7 Abs. 3 DSG 2000 normierten Verhältnismäßigkeitsgrundsatzes: Wenn es denkmöglich ist, dass die von einer in der Sache zuständigen Behörde ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet sind, ist die Zulässigkeit der Ermittlung aus datenschutzrechtlicher Sicht gegeben.« (Bescheid der Datenschutzkommission vom 29. 11. 2005, K121.046/0016-DSK/2005)

Eine solche überschießende Datenverwendung im Sinne der zitierten ständigen Rechtsprechung (zu den Generalklauseln des § 8 DSG 2000), die mit dem gesetzmäßigen Zweck nicht mehr für jedermann einsichtig begründet werden kann, liegt hier aber nicht vor. Die Beschwerdegegnerin hat die Ermächtigung gem § 5c Abs. 4 Z 2 Oö. JWG 1991 nicht überschritten. Der Beschwerde war daher als unbegründet abzuweisen.

l. Übermittlung von Daten an das Pflegschaftsgericht (K121.833/0008-DSK/2012, 14. 9. 2012)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass die Beschwerdegegnerin (eine Bundespolizeidirektion) gegen ihn ein Verwaltungsstrafverfahren eingeleitet und dem Pflegschaftsgericht – der Beschwerdeführer ist minderjährig und, eigenen Angaben zu Folge, schwer geistig behindert – die näheren Umstände des Verfahrens schriftlich mitgeteilt habe. Die ihm zuvor als Zulassungsbesitzer eines Kfz zugestellte Aufforderung zur Erteilung einer Lenkerauskunft sei rechtswidrig erfolgt. Auf diesen Einwand im Verwaltungsstrafverfahren habe die Beschwerdegegnerin bei Gericht wegen des Vorliegens einer pflegschaftsgerichtlichen Genehmigung für die Kfz-Zulassung nachgefragt und dabei ohne irgendeine Veranlassung Daten aus dem anhängigen Verwaltungsstrafverfahren übermittelt.

Bei der Beschwerdegegnerin als Verwaltungsstrafbehörde wurde wegen einer von privater Seite angezeigten Übertretung der StVO (unerlaubtes Parken), die vom Lenker des Pkw mit bekannten Kennzeichen im Februar 2011 begangen wurde, ermittelt. Für dieses Kfz war der Beschwerdeführer seit Dezember 2007 Zulassungsbesitzer. Er wurde daher im März 2011 gem § 103 Abs. 2 KFG aufgefordert, über den Lenker im Zeitpunkt der Übertretung oder die sonst auskunftspflichtige Personen Auskunft zu erteilen. Der rechtsfreundliche Vertreter des Beschwerdeführers teilte daraufhin mit, dass dieser schwer psychisch behindert, zu 80 % invalide und Schüler einer Behindertenschule ist. Er sei in Folge seiner Krankheit nicht in der Lage, die geforderte Auskunft zu erteilen und überdies nicht schuldfähig. Da die Ermittlung des verantwortlichen Lenkers für die im Februar 2011 mit dem Kfz des Beschwerdeführers

begangene Verwaltungsübertretung in weiterer Folge nicht zeitgerecht möglich war, wurde das Verwaltungsstrafverfahren wegen Verjährung im August 2011 eingestellt. Im November 2011 richtete die Beschwerdegegnerin an das für den Beschwerdeführer zuständige Pflegschaftsgericht folgendes (wesentliches) Schreiben:

»... Mitteilung an das zuständige Pflegschaftsgericht über die Zulassung eines Kraftfahrzeugs auf eine minderjährige Person (§ 154 Abs. 3 ABGB)

Im Ermittlungsverfahren des ha. geführten Verwaltungsstrafverfahrens [...] wurde festgestellt, dass am [...]12.2007 auf den damals 11-jährigen [Beschwerdeführer] das Kfz [...] angemeldet wurde.

Im Schreiben des Bundesministeriums für Justiz vom [...]2010 an das BMfVIT mit dem Bezug [...] wurde erörtert, dass im Hinblick auf die Anmeldung von Kfz auf Personen unter 14 Jahren eine solche pflegschaftsgerichtlich genehmigt werden muss, wenn diese dem ordentlichen oder außerordentlichen Wirtschaftsbetrieb des Minderjährigen zuzuordnen ist: [...In der Regel wird die Anmeldung eines Kraftfahrzeugs auf einen Minderjährigen, das dieser nicht selbst lenkt, nicht im Rahmen des ordentlichen Wirtschaftsbetriebs erfolgen. Anderes könnte gelten, wenn ein Minderjähriger etwa ein Mietwagenunternehmen im Erbweg erwirbt, im Rahmen eines derartigen Unternehmens kann die Anmeldung von Kraftfahrzeugen wohl üblicherweise dem ordentlichen Wirtschaftsbetrieb zugerechnet werden.]

Aufgrund des im Ermittlungsverfahren zu [...] aktenkundig gewordenen und mit ärztlichen Attesten bewiesenen psychischen Gesundheitszustand des [Beschwerdeführer], vertreten durch dessen Mutter [...] (schwere psychische Behinderung, Schizophrenie mit Wahnvorstellungen, etc.) ist es sehr unwahrscheinlich, dass im Jahr 2007 die Anmeldung des Kraftfahrzeugs auf den damals 11-jährigen [Beschwerdeführer] im Rahmen des ordentlichen Wirtschaftsbetriebs erfolgte.

Daher verbleibt es dem Bezirksgericht [...] als Pflegschaftsgericht zunächst zu überprüfen, ob die damalige Anmeldung des Kraftfahrzeugs der pflegschaftsgerichtlichen Genehmigung bedurft hat und ob eine solche gemäß § 154 Abs. 1 ABGB vorher eingeholt wurde. ...«

Das Bezirksgericht eröffnete daraufhin ein den Beschwerdeführer betreffendes pflegschaftsgerichtliches Verfahren.

Rechtliche Würdigung:
Die gegenständliche Datenübermittlung war eine solche per Briefpost. Eine Verletzung des Rechts auf Geheimhaltung war demnach anhand des Grundrechts zu prüfen, wobei, da es sich um Daten betreffend ein Verwaltungsstrafverfahren handelt, § 8 Abs. 4 DSG 2000 sinngemäß anzuwenden ist.

Gem § 21 Abs. 1 ABGB stehen Minderjährige und in ihrer Geschäftsfähigkeit aus anderen Gründen beschränkte Personen unter dem besonderen Schutz der Gesetze. Daraus folgt, dass jede Behörde angewiesen ist, die Rechte und Interessen Minderjähriger zu schützen und wahrzunehmen, so dem nicht eindeutig andere gesetzliche Vorschriften entgegenstehen. Dies gilt ganz besonders für den Beschwerdeführer, bei dem zur Minderjährigkeit noch eine schwere psychische, seine Geschäftsfähigkeit beeinträchtigende Krankheit kommt.

Die Wahrnehmungen der Beschwerdegegnerin im Verwaltungsstrafverfahren begründeten, auch ohne dass es dafür eines Rückgriffs auf die nur intern maßgeblichen Erlässe und Rechtsmeinungen der Bundesministerien bedurfte, den Verdacht, dass die für den Beschwerdeführer Obsorge- und Vertretungsberechtigten nicht im Einklang mit den zum Wohle Minderjähriger

geltenden Gesetzen gehandelt haben, indem sie ihn als Privatperson (ohne Zusammenhang mit einem Unternehmen) als Zulassungsbesitzer eines Kfz (und damit als die vorrangig zivil- wie strafrechtlich für das Kfz und dessen Betrieb haftbare Person) eintragen ließen, ohne vorher eine pflegschaftsgerichtliche Genehmigung erwirkt zu haben.

Es war daher klar im Interesse des Beschwerdeführers, dem zuständigen Pflegschaftsgericht von dieser Tatsache Kenntnis zu verschaffen, damit es zum Wohle des Beschwerdeführers einschreiten konnte. Dass das Bezirksgericht dabei bloß durch Gebrauch der Worte »Verwaltungsstrafverfahrens« und »Beschuldigten« davon Kenntnis erlangte, dass der Beschwerdeführer als Bezugsperson in ein Verwaltungsstrafverfahren involviert war, wiegt als Eingriff in das Grundrecht auf Datenschutz im Vergleich zu seinen oben dargestellten rechtlich geschützten Interessen weniger schwer. In diesem Zusammenhang sei erwähnt, dass der Beschwerdeführer stets nur als auskunftspflichtiger Zulassungsbesitzer und nicht als Beschuldigter behandelt wurde, da gegen ihn nie eine Verfolgungshandlung iSd § 32 Abs. 2 VStG gesetzt wurde.

Dabei ist in Rechnung zu stellen, dass Kenntnis von den näheren Umständen, die die Einbeziehung des Beschwerdeführers in das Verwaltungsstrafverfahren bewirkt haben, für das Pflegschaftsgericht durchaus von Interesse sein könnte.

In sinngemäßer Anwendung des § 8 Abs. 4 DSG 2000 konnte sich das Vorgehen der Beschwerdegegnerin daher auf die Ziffern 2 und 3 der zitierten Gesetzesbestimmung stützen. Das Handeln der Beschwerdegegnerin war hier sogar nicht nur gemäß überwiegender berechtigter Interessen der Beschwerdegegnerin, sondern wegen überwiegender eigener Interessen des Beschwerdeführers gestattet, da er – sogar zweifach, wegen Minderjährigkeit und einer geistigen Behinderung – zum Kreis der gem § 21 Abs. 1 ABGB »unter dem besonderen Schutz der Gesetze« stehenden Personen gehört. Durch die in Beschwerde gezogene Datenübermittlung wurde es dem mit der Wahrnehmung dieses Schutzes in Fragen der rechtsgeschäftlichen Vertretung betrauten Bezirksgericht überhaupt erst möglich, diese Interessen des Beschwerdeführers wahrzunehmen.

Die Beschwerde war daher als unbegründet abzuweisen.

m. Verwendung von Meldedaten für Meinungsumfrage (K121.879/0014-DSK/2012, 14. 12. 2012)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung in den Rechten auf Geheimhaltung und Löschung durch den Magistrat der Stadt Graz. Dieser habe seine Daten aus dem Melderegister bzw. der Wählerevidenz unrechtmäßig dazu verwendet, eine unzulässige und datenschutzrechtlich bedenkliche Bürgerbefragung vorzubereiten, bei der die Teilnehmer irreführend in dem Glauben gelassen werden, die Teilnahme erfolge anonym. Alle Stimmabgaben müssten jedoch unter Verwendung eines persönlichen Codes und unter Angabe des Geburtsdatums erfolgen. Auch sei es möglich, diese beiden Daten bei brieflicher Stimmabgabe während des Postlaufs von Briefumschlägen abzulesen und bei der parallel laufenden Online-Abstimmung nochmals zu verwenden bzw. die briefliche Stimmabgabe zu unterlaufen und zu manipulieren. Der Widerspruch des Beschwerdeführers dagegen bzw. sein Löschungsbegehren seien abgelehnt worden.

Die Landeshauptstadt Graz führte auf Beschluss des Stadtsenats gemäß den »Richtlinien für Grazer BürgerInnenumfragen« im Juli 2012 eine allgemeine Meinungsumfrage zu zwei Fragen der Kommunalpolitik durch. Teilnahmeberechtigt waren alle Personen, unabhängig von ihrer Staatsangehörigkeit, die zum Stichtag das 16. Lebensjahr vollendet hatten und mit

Hauptwohnsitz in Graz gemeldet waren. Der Beschwerdegegner war mit der organisatorischen Durchführung dieser Meinungsumfrage beauftragt.

Die Daten der Teilnahmeberechtigten, darunter auch die des Beschwerdeführers, wurden anhand der oben dargestellten Kriterien (Geburtsdatum, Hauptwohnsitz am Stichtag) aus dem lokalen Melderegister ausgewählt. In einem weiteren Schritt wurde jedem Teilnahmeberechtigten ein 16-stelliger numerischer Code (Teilnehmercode) zugeordnet. Durch die Verwendung dieses Codes wurde sichergestellt, dass jeder Teilnahmeberechtigte seine Meinung nur einmal bekannt geben konnte. Nach Erfassung dieses Codes in dem zur Auswertung der Umfrage verwendeten EDV-Programm wurde jeweils die Meinungsbekanntgabe (das Votum) gezählt und statistisch erfasst, der Teilnahmeberechtigte jedoch für ein weiteres Votum gesperrt.

Alle Teilnahmeberechtigten, darunter auch der Beschwerdeführer, erhielten ein Schreiben des Beschwerdegegners mit Informationen zu den Themen der Umfrage, einem Befragungsblatt, einem mit einem Strichcode/Barcode versehenen Rückantwortkuvert und dem Teilnehmercode.

Der Beschwerdeführer gab sein Votum in einer Servicestelle des Beschwerdegegners persönlich ab. Dazu musste er sich mit einem amtlichen Lichtbildausweis sowie dem Teilnehmercode identifizieren und durch seine Unterschrift und Angabe des Teilnehmercodes in einer mit »BürgerInnenumfrage 2012 – Datenschutzerklärung« betitelten Liste folgende Erklärung abgeben:

»Mit meiner Unterschrift erkläre ich mich im Sinne von § 8 Abs. 1 Z 2 Datenschutzgesetz damit einverstanden, dass meine persönlichen Daten (Name, Adresse und Geburtsdatum) für die elektronische Verarbeitung meiner Teilnahme verwendet werden.«

Anschließend wurde seine Teilnahme durch Verarbeitung des Teilnehmercodes registriert, sein Befragungsblatt mit dem Votum entgegengenommen und für das Befragungsergebnis gezählt. Eine Verarbeitung des Inhalts des Votums gemeinsam mit den Personendaten des Beschwerdeführers, die die Meinungsäußerung des Beschwerdeführers nachvollziehbar gemacht hätte, ist nicht erfolgt.

Sein Widerspruch- und Löschungsbegehren lehnte der Beschwerdegegner aufgrund der irreversiblen Datenverwendung auf Grundlage der Zustimmungserklärung aus Datenschutzgründen und technischer Unmöglichkeit ab. Jene Daten, die eine Teilnahme des Beschwerdeführers an der Umfrage nachweisen (Vor-, Familienname, Geburtsdatum und Anschrift, Teilnehmercode, Faktum der Teilnahme) wurden im August 2012 gelöscht und dies dem Beschwerdeführer mitgeteilt. Die »Streichung Ihrer Stimme selbst« wurde wiederum abgelehnt.

Rechtliche Würdigung:
Da es sich beim Handeln des Beschwerdegegners im Juli 2012 um keinen hoheitlich Vollziehungsakt der direkten Demokratie (Volksabstimmung oder Volksbefragung), insb um keine Abstimmung oder Befragung nach dem Steiermärkischen Volksrechtegesetz (LGBl. Nr 87/1986 idgF) gehandelt hat, wurden Begriffe, die der Umfrage den Charakter einer Volksabstimmung oder Volksbefragung verleihen könnten, vermieden.

Die im Vorbringen des Beschwerdeführers aufgeworfenen Fragen, ob die Grundsätze der Datensicherheit gem § 14 DSG 2000 eingehalten wurden oder das Befragungsverfahren gegen Manipulationen in jeder Hinsicht gesichert war (siehe die vom Beschwerdeführer aufgeworfene Frage, ob ein briefliches Votum mithilfe der auf dem Rückantwortkuvert außen anzubringenden Daten »Geburtsdatum« und »Teilnehmercode« per Online-Votum »unterlaufen« werden könnte), machen kein subjektiv-öffentliches, vor der Datenschutzkommission im Beschwerdeverfahren nach § 31 DSG 2000 durchzusetzendes Recht des Beschwerdeführers geltend.

Zum Recht auf Geheimhaltung: In diesem Punkt hat sich die Beschwerde als berechtigt erwiesen. Meldedaten dürfen aufgrund der Bestimmung des § 20 Abs. 3 MeldeG an Organe der Gebietskörperschaften nur übermittelt werden, wenn das Verlangen auf Übermittlung für den Empfänger zur Wahrnehmung der »ihm übertragenen Aufgaben« eine wesentliche Voraussetzung bildet bzw. dürfen die Bürgermeister die in ihrem Melderegister enthaltenen oder ihnen gem § 20 Abs. 2 leg cit übermittelten Meldedaten nur verwenden, sofern diese zur Wahrnehmung der »ihnen gesetzlich übertragenen Aufgaben« eine wesentliche Voraussetzung bilden. Wenngleich der erste Satz – im Gegensatz zum letzten Satz – des § 20 Abs. 3 MeldeG nur von »übertragenen Aufgaben« und nicht von »gesetzlich übertragenen Aufgaben« spricht, ist auch diese Bestimmung aus nachstehenden Gründen im letzteren Sinne zu verstehen:

§ 20 Abs. 3 MeldeG in seiner Stammfassung, BGBl. Nr. 9/1992, lautete wie folgt:

»(3) Organen der Gebietskörperschaften sind auf Verlangen die im Melderegister enthaltenen Meldedaten zu übermitteln, sofern diese für den Empfänger zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bilden. Die Bürgermeister sind ermächtigt, die in ihrem Melderegister enthaltenen oder ihnen gemäß Abs. 2 übermittelten Meldedaten zu verwenden, sofern diese zur Wahrnehmung der ihnen gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bilden.«

Durch Art. IZ 16 des Hauptwohnsitzgesetzes, BGBl Nr. 505/1994, erhielt der erste Satz des § 20 Abs. 3 MeldeG folgende Fassung:

»Organen der Gebietskörperschaften sind auf Verlangen die im Melderegister oder im Zentralen Melderegister enthaltenen Meldedaten zu übermitteln, sofern diese für den Empfänger zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bilden; Übermittlungen auf Grund von Verknüpfungsanfragen (§ 16 Abs. 1) sind überdies nur zulässig, wenn die Verhältnismäßigkeit zum Anlass und zum angestrebten Erfolg gewahrt bleibt.«

Im Jahre 2001 wurden zwei Novellen des MeldeG im BGBl – und zwar beide unter BGBl. I Nr. 28/2001 – kundgemacht. Beide enthielten eine Änderung des § 20 Abs. 3 MeldeG. Art. I Z 14 des Bundesgesetzes, mit dem das Meldegesetz 1991, das Volkszählungsgesetz 1980 und das Allgemeine Sozialversicherungsgesetz geändert wurden, ersetzte das Klammerzitat »(§ 16 Abs. 1)« durch das Klammerzitat »(§ 16a Abs. 3)«. Art. II Z 15 desselben Gesetzes lautete in Bezug auf § 20 Abs. 3 MeldeG wie folgt:

»In § 20 Abs. 3 wird die Wortfolge »zu übermitteln, sofern diese für den Empfänger zur Wahrnehmung der ihm übertragenen Aufgaben eine wesentliche Voraussetzung bildet« ersetzt durch »zu übermitteln, wobei das Verlangen im konkreten Fall nur gestellt werden darf, wenn es für den Empfänger zur Wahrnehmung der ihm übertragenen Aufgaben eine wesentliche Voraussetzung bildet«.

Aus diesem Wortlaut ist ersichtlich, dass dem Gesetzgeber insofern ein Irrtum unterlaufen ist, als er übersehen hat, dass der erste Satz des § 20 Abs. 3 leg.cit. das Wort »gesetzlich« enthält. Die Änderung selbst geht auf einen Abänderungsantrag des Ausschusses für innere Angelegenheiten zurück (Bericht des Ausschusses für innere Angelegenheiten über die Regierungsvorlage (424 der Beilagen) und wurde wie folgt begründet:

»Zu Art. II § 20 Abs. 3 MeldeG: Die Änderung berücksichtigt, dass bei Online-Amtshilfe die Kontrollmöglichkeit des Auskunftgebers eingeschränkt ist. Es wird daher vorgeschlagen, die Verantwortlichkeit für die Zulässigkeit der Anfrage auf den Anfragenden zu überbinden.«

Aus dieser Entstehungsgeschichte ist klar ersichtlich, dass es nicht im Willen des Gesetzgebers gelegen ist, Organen der Gebietskörperschaften – im Gegensatz zu den datenschutzrechtlichen Befugnissen der Bürgermeister – Meldedaten auch dann zu überlassen, wenn diese nicht zur Wahrnehmung einer ihnen »gesetzlich übertragenen Aufgabe« erfolgt. Die gegenteilige Auffassung würde überdies dem letzten Satz des § 20 Abs. 3 MeldeG inhaltsleer machen, was auch nicht dem gesetzgeberischen Willen unterstellt werden kann. Es ist daher davon auszugehen, dass im Anwendungsbereich des § 20 Abs. 3 MeldeG in jedem Fall – sei es für die Wahrnehmung von Aufgaben eines Organs einer Gebietskörperschaft, sei es für die Wahrnehmung von Aufgaben der Bürgermeister – die Aufgabe, für deren Erfüllung die Meldedaten verwendet werden sollen, eine »gesetzlich übertragene Aufgabe« sein muss.

Die Durchführung einer als Akt der Privatwirtschaftsverwaltung deklarierten, weil außerhalb des Steiermärkischen Volksrechtegesetzes abgeführten Meinungsumfrage, die sich bloß auf eine auf der Grundlage des § 45 Abs. 6 des Statuts der Landeshauptstadt Graz 1967 vom Gemeinderat erlassenen Richtlinie stützt, kann nicht als eine dem Beschwerdegegner noch einem sonstigen Organ dieser Stadt gesetzlich übertragene Aufgabe angesehen werden. Würde man nämlich alle im Rahmen des eigenen Wirkungsbereiches einer Gemeinde wahrzunehmenden Aufgaben – also auch die gesamte Privatwirtschaftsverwaltung – als »gesetzlich übertragene Aufgaben« ansehen, gäbe es in diesem Wirkungsbereich keine anderen als nur gesetzlich übertragene Aufgaben.

Es war daher gem § 31 Abs. 7 DSG 2000 ein Eingriff in das Geheimhaltungsrecht des Beschwerdeführers, welches auch ein Verbot der unzulässigen Verwendung von Daten für ein anderes Aufgabengebiet beinhaltet, festzustellen.

Zum Recht auf Löschung: Soweit für Zwecke der Durchführung der Befragung direkt personenbezogene Daten (Vor-, Familienname, Geburtsdatum und Anschrift, Teilnehmercode, Faktum der Abgabe eines Votums in der Befragung) verwendet worden sind, wurden diese nach Abschluss der Auswertung der Umfrage gelöscht. Damit entfällt jedenfalls eine Beschwer, da das Löschungsbegehren erfüllt wurde. Die Beschwerde war diesbezüglich abzuweisen.

Soweit es um das Votum selbst geht, hat die Sachverhaltsfeststellung ergeben, dass nicht mehr nachvollzogen werden kann, wie der Beschwerdeführer gestimmt hat, dh, welchen Inhalt seine Meinungsäußerung hatte. Das Votum ist zwar in die Auswertung (Zählung, statistische Erfassung) der Umfrage eingegangen, kann daher aber schon aus diesem technischen Grund nicht mehr inhaltlich abgeändert oder auf Wunsch eines Betroffenen aus der Statistik herausgelöst werden.

Die Beschwerde war daher hinsichtlich des Löschungsrechts als unbegründet abzuweisen.

n. Übermittlung eines Bescheids im Sozialversicherungsbereich (K121.891/0003-DSK/2013, 18. 1. 2013)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass die Beschwerdegegnerin (eine Gebietskrankenkasse) einen Feststellungsbescheid aus April 2012 betreffend eines Vollversicherungsverhältnisses aufgrund von Tätigkeit als Dienstnehmer von 2007 bis 2010 nicht nur an Dienstnehmer und Dienstgeber, sondern auch an das (lokale) Finanzamt, eine Kreditauskunftei, ein Bezirksgericht sowie eine Landesgeschäftsstelle des Arbeitsmarktservice (AMS) zugestellt habe. Der Bescheid sei nicht rechtskräftig, da er dagegen Berufung erhoben habe. Überdies habe er im Mai 2012 von der Beschwerdegegnerin die Löschung bzw. Richtigstellung von Daten verlangt.

Der Beschwerdeführer steht unter dem Verdacht der mehrfachen Verletzung abgabenrechtlicher, sozialversicherungsrechtlicher und insolvenzrechtlicher Pflichten. Er ist seit 2005 als arbeitssuchend gemeldet und bezog über das AMS Leistungen aus der Arbeitslosenversicherung. Jedenfalls von 2007 bis 2010 stand er als Buchhalter in einem Dienstverhältnis zu einem Steuerberater, wurde aber nicht zur Sozialversicherung angemeldet sondern bezog Entgelt in Form von Stundensätzen auf »Werkvertragsbasis«, wofür er Rechnungen unter Angabe einer (Nicht-Wohn-)Adresse in der Schweiz legte, und das auf ein Konto bei einer Bank in der Schweiz überwiesen wurde.

Mit Beschluss aus Mai 2007 wurde vom Bezirksgericht ein Schuldenregulierungsverfahren betreffend das Vermögen des Beschwerdeführers eröffnet. Im August 2007 wurde ein Abschöpfungsverfahren eingeleitet und eine Kreditauskunftei als Treuhänder und Beteiligter bestimmt. Im August 2007 wurde das Schuldenregulierungsverfahren aufgehoben.

Im Zuge einer gemeinsamen Prüfung lohnabhängiger Abgaben in der Steuerberatungskanzlei wurde vom Prüfer erhoben, dass der Beschwerdeführer regelmäßig Entgelte auf Basis von Stundensätzen und Stundenlisten verrechnete. Es fielen weiters Zahlungen an den Beschwerdeführer ohne Belege auf. Dies wurde an die Beschwerdegegnerin übermittelt, die ein entsprechendes Ermittlungsverfahren betreffend Bestehen einer ASVG-Pflichtversicherung (und, daraus folgend, evtl Vorschreibung nicht entrichteter Beiträge zur Sozialversicherung an die Beteiligten) einleitete. Bei einer angesetzten Vernehmung im Juli 2011 verweigerte der Beschwerdeführer die Aussage, worauf sich die Beschwerdegegnerin Akteneinsicht in einem parallelen kriminalpolizeilichen Ermittlungsverfahren verschaffte, insb in die Beschuldigtenvernehmung des Beschwerdeführers aus Oktober 2010, die, neben den Ergebnissen der GPLA, zur Sachverhaltsfeststellung in wesentlichen Punkten herangezogen wurde.

Im April 2012 stellte die Beschwerdegegnerin das Bestehen einer sozialversicherungsrechtlichen Pflichtversicherung (ASVG-Vollversicherung und Arbeitslosenversicherung) des Beschwerdeführers als Dienstnehmer im Zeitraum 2007 bis 2010 bescheidmäßig fest. Dieser Bescheid wurde nicht sofort rechtskräftig, da der Beschwerdeführer dagegen Einspruch erhoben hat, und (nachweislich, RSb) an den Beschwerdeführer und den Dienstgeber sowie »nachrichtlich« an das Finanzamt, die Kreditauskunftei, das Bezirksgericht sowie das AMS übermittelt.

Im Mai 2012 verlangte der Beschwerdeführer von der Beschwerdegegnerin unter Bezugnahme auf den Bescheid vom April 2012, die betroffenen Daten zu löschen/berichtigen und ihn davon zu verständigen. Nähere Angaben, was mit den »betroffenen Daten« gemeint sei, enthält das Schreiben nicht. Die Beschwerdegegnerin reagierte darauf innerhalb der Achtwochenfrist nicht. Erst im bereits anhängigen datenschutzrechtlichen Beschwerdeverfahren wurde dem Beschwerdeführer im September 2012 mitgeteilt, dass sein Begehren abgelehnt werde, da man auf dem Standpunkt stehe, alle Daten rechtmäßig ermittelt zu haben und eine Abänderung von Akteninhalten schon im Hinblick auf ein anhängiges Rechtsmittelverfahren aus Gründen der Dokumentationspflicht nicht zulässig sei. Dieses Ablehnungsschreiben wurde dem Beschwerdeführer zugestellt.

Rechtliche Würdigung:

A. Hinsichtlich der Ermittlung der Daten verwies die Datenschutzkommission auf ihre ständige Rechtsprechung, wonach die inhaltliche Überprüfung des Ermittlungsverfahrens einer sachlich zuständigen Behörde durch die Datenschutzkommission auf Fälle von Ermittlungsexzessen (überschießende, denkmöglich nicht erforderliche Datenermittlung) beschränkt ist (»... verbleibt für die Datenschutzkommission das Übermaßverbot als Ausdruck des in § 1 Abs. 2 und § 7 Abs. 3 DSG 2000 normierten Verhältnismäßigkeitsgrundsatzes: Wenn es denkmöglich ist,

dass die von einer in der Sache zuständigen Behörde ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet sind, ist die Zulässigkeit der Ermittlung aus datenschutzrechtlicher Sicht gegeben.« (Bescheid vom 29. November 2005, GZ: K121.046/0016-DSK/2005).

Im Beschwerdefall vermochte der Beschwerdeführer nichts aufzuzeigen, was eine überschießende, der Sache (Verfahrensgegenstand, Beweisthemen) nicht gerecht werdende Datenermittlung auch nur zu bescheinigen vermag. Wie die Beschwerdegegnerin zutreffend ausführte, war und ist sie insb durch § 41a ASVG ermächtigt, für mehrfache gesetzmäßige Zwecke (Einhaltung von Vorschriften des Sozialversicherungsrechts, Einhaltung der auf die Lohnsteuerverrechnung und -abfuhr bezogenen Bestimmungen des EStG 1988), dh auch für die Abgabenbehörden und für das AMS als für die Verwaltung der Arbeitslosenversicherung zuständiger Behörde, Prüfungen von Dienstgebern durchzuführen, wobei im konkreten Fall die Ergebnisse auch in Bezug auf den Beschwerdeführer insofern relevant waren, als dieser, obwohl nach dem nicht rechtskräftigen Verfahrensstand in einem eine Vollversicherung in der Sozialversicherung begründenden Dienstverhältnis stehend, jahrelang keine Dienstnehmeranteile an Sozialversicherungsbeiträgen bezahlt hatte. Ob er für die »brutto für netto« erhaltenen Entgelte, die auf ein Konto in der Schweiz überwiesen wurden, im Inland Einkommensteuer bezahlt hatte, war nicht bekannt, Lohnsteuer wurde jedenfalls nicht verrechnet und einbehalten. Daneben war bekannt, dass der Beschwerdeführer, beim AMS als arbeitsuchend gemeldet, Leistungen der Arbeitslosenversicherung beansprucht hat.

Da der Beschwerdeführer laut Sachverhaltsfeststellungen keine niederschriftliche Aussage zu den Ergebnissen der Prüfung machen wollte, war die Beschwerdegegnerin berechtigt, in Geltendmachung ihres Anspruchs auf Rechts- und Verwaltungshilfe (§ 360 Abs. 1 ASVG) Einsicht in die Akten des gegen den Beschwerdeführer bereits anhängigen kriminalpolizeilichen Ermittlungsverfahrens zu nehmen und dessen dortige Aussage als Beweismittel zu verwerten. Dies kann weder als überschießend gewertet werden, noch liegt damit eine Verletzung des Grundsatzes der Zweckbindung einer Datenverwendung gem § 6 Abs. 1 Z 2 DSG 2000 vor, da sich dieses Vorgehen der Beschwerdegegnerin auf gesetzliche Ermächtigungen stützen kann.

Der Beschwerdegegnerin fällt daher kein Ermittlungsexzess zu Last. Zu beurteilen, ob einzelne Beweisaufnahmen für Zwecke des erlassenen Bescheids zulässig waren, fällt in die Zuständigkeit der (Rechtsmittel-)Behörden im sozialversicherungsrechtlichen Verwaltungsverfahren.

B. Zur Übermittlung des Bescheids wurde ausgeführt, dass sich aus § 321 Abs. 1 ASVG (siehe auch § 360 Abs. 7 ASVG) eine besonders starke wechselseitige Hilfs- und Unterstützungspflicht zwischen Sozialversicherungsträgern und Abgabenbehörden ergibt. Aus besagter Bestimmung folgt, dass diese Behörden einander auch gegenseitig unaufgefordert Informationen zukommen lassen müssen, die für das Aufgabengebiet des jeweiligen Empfängers von Bedeutung sind. § 321 Abs. 1 3. Satz ASVG stellt ausdrücklich klar, dass diese Ermächtigung auch für Datenübermittlungen gilt.

Daraus folgt zunächst, dass eine Zustellung des Bescheids aus April 2012 an das Finanzamt zulässig, ja sogar ausdrücklich gesetzlich geboten war. Dieses Finanzamt hat insb zu entscheiden, ob der Beschwerdeführer seinen Pflichten gem EStG 1988 entsprochen hat. Eine gleichwertige Ermächtigung enthält § 69 Abs. 1 AlVG betreffend Datenübermittlung an das AMS.

Die Bestimmung des § 321 Abs. 1 ASVG ist jedoch nicht auf das Bezirksgericht und die Kreditauskunftei als Treuhänder anwendbar. Auch die Anwendung von § 42 Abs. 4 ASVG scheidet aus, da zu den dort angeführten Zwecken (Rechtsgebieten) nicht das Insolvenzrecht zählt.

Zwar liegt hier eine ähnliche Interessenlage vor (der Beschwerdeführer hat möglicherweise gegen seine Obliegenheiten gem § 210 IO gehandelt, das Gesetz sieht hier, bei einem Eingriff einer staatlichen Behörde iSd Art. 8 EMRK (wenn auch in Form eines Selbstverwaltungsträgers), aber keine ausdrückliche Ermächtigung im Sinne der Verfassungsbestimmung des § 1 Abs. 2 DSG 2000 vor, um ohne entsprechende Aufforderung einer zur Inanspruchnahme einer Amtshilfeleistung der Beschwerdegegnerin berechtigten Stelle Daten, die zum Inhalt des Bescheids gehörten, an das Bezirksgericht und die Kreditauskunftei zu übermitteln.

Der Beschwerde war daher insoweit Folge zu geben.

C. Zum Recht auf Löschung/Richtigstellung wurde ausgeführt, dass ein Bescheid einer Verwaltungsbehörde und das diesem zugrunde liegende gesetzliche Ermittlungsverfahren keine »Datenanwendung« iSd § 4 Z 7 DSG 2000 darstellt. Eine Abänderung von Bescheiden anderer Behörden durch die Datenschutzkommission bzw. ein Auftrag der Datenschutzkommission an eine andere Verwaltungsbehörde, einen Bescheid abzuändern, ist rechtlich nicht möglich. Weder der Spruch eines Bescheids noch die Sachverhaltsfeststellungen oder andere Teile einer Bescheidbegründung unterliegen einer Löschung oder Richtigstellung gem § 27 DSG 2000, auch wenn der entsprechende Text, wovon auszugehen ist, mithilfe automationsunterstützter Datenverarbeitung erstellt worden ist.

Dies ergibt sich nicht nur aus verfassungsrechtlichen Grundsätzen (Art. 83 Abs. 2 B-VG, Recht auf den gesetzlichen Richter, dh auf Entscheidung einer einzigen, durch Gesetz festgelegten, zuständigen Behörde) sondern auch einfachgesetzlich aus dem in § 27 Abs. 3 DSG 2000 vorgesehenen Dokumentationszweck bestimmter Datenanwendungen (z. B. solchen zur Verfahrensführung, elektronischen Aktenführung und Dokumentation, Kanzleitätigkeit etc.).

Als »richtig« gelten Daten, die für diesen Zweck verwendet werden, wenn sie das Ergebnis des Ermittlungsverfahrens und die Entscheidung der Behörde formell richtig wiedergeben. Auf die rechtliche Richtigkeit der Entscheidung sowie auf die inhaltliche Aussagekraft oder den Wert von Beweismitteln (z. B. den Inhalt einer Niederschrift oder eines Sachverständigengutachtens) kommt es in diesem Zusammenhang hingegen nicht an. All dies kann und darf nicht im Rahmen eines datenschutzrechtlichen Verfahrens überprüft werden.

Überdies erfordert ein Löschungsbegehren gem § 27 Abs. 1 Z 2 DSG 2000 ein höheres Maß an Präzisierung, als es der Beschwerdeführer in seinem Schreiben vom Mai 2012 (sinngemäß lautete dieses einfach, alle für den Zweck der Erstellung des Bescheids vom April 2012 verarbeiteten Daten zu löschen bzw. richtigzustellen) zum Ausdruck gebracht hat. Im Fall eines Richtigstellungsbegehrens hat der Betroffene insb genau auszuführen, bei welchen Datenarten Inhalte durch andere, vom Betroffenen anzugebende Inhalte zu ersetzen wären.

Aus diesen Gründen hat die Beschwerdegegnerin das Löschungs- und Richtigstellungsbegehren des Beschwerdeführers mit Schreiben aus September 2012 zwar verspätet, aber doch zu Recht abgelehnt. Die Beschwerde war diesbezüglich abzuweisen.

o. Abfrage im ZMR rechtswidrig (K121.894/0003-DSK/2013, 18. 1. 2013)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung durch eine ZMR- und EKIS-Abfrage durch eine Bundespolizeidirektion (Beschwerdegegnerin). Er habe im Juni 2012 bei einer staatlichen Vereinigung beim Portier ein Konvolut für deren Präsidenten abgegeben, welches nur ihm persönlich ausgehändigt werden sollte. Er habe um Antwort ersucht und daher auf eine postalische Antwort gewartet, im Juli 2012 allerdings ein Schreiben der (örtlichen)

Bundespolizeidirektion mit dem Betreff »Ausfolgung von sichergestellten Gegenständen« erhalten und sei aufgefordert worden, beim Polizeikommissariat zu erscheinen. Dort sei ihm erklärt worden, dass das Konvolut für eine Briefbombe gehalten und daher untersucht worden sei. Der Beschwerdeführer habe am selben Tag Kopien eines Polizeiberichts erhalten, welcher diese Aussage bestätigt habe. Die Polizei habe das Konvolut letztlich für unbedenklich gehalten. Da sich im Konvolut ein Lebenslauf des Beschwerdeführers befunden habe, seien rechtswidrigerweise eine ZMR- und eine EKIS-Anfrage durchgeführt worden, obwohl bereits festgestellt worden sei, dass das Konvolut keine Bombe und keine Drohung oder Forderung enthalten habe.

Nach Übergabe des adressierten (Empfänger wie Absender) Briefkuverts mit Vermerken (etwa »Bote«, »Künstlerpost«, »Querdenker«) an den Portier im Haus der staatlichen Vereinigung führte die Beschwerdegegnerin einen Einsatz durch. Den vor Ort einschreitenden Beamten wurde das Paket des Beschwerdeführers gezeigt und die Vermutung geäußert, dass es sich um eine Briefbombensendung handeln könnte. Da die einschreitenden Beamten dies ihrerseits nach Durchführung eines Augenscheins nicht völlig ausschließen konnten, wurde ein sprengstoffkundiges Organ angefordert, welches das Paket sowie das Kuvert öffnete. In dem Kuvert befand sich – neben anderen Dokumenten mit teilweise unzusammenhängenden Aussagen sowie diversen Fotos – auch ein Lebenslauf des Beschwerdeführers. Im Juni 2012 wurde im Zuge der Anfertigung des Einsatzberichtes festgestellt, dass im PAD eine weitere Wohnadresse des Beschwerdeführers aufschien, weshalb eine Abfrage im ZMR zur Person des Beschwerdeführers durchgeführt wurde, um eine Zustelladresse zu ermitteln. Der ZMR-Auszug zeigt sämtliche Wohnsitze des Beschwerdeführers von 1976 bis zum Zeitpunkt der Abfrage. Eine ebenfalls zur Person des Beschwerdeführers durchgeführte Abfrage im EKIS zum Zweck der Gefahrenerforschung verlief negativ.

Rechtliche Würdigung:
Die Beschwerde hat sich als teilweise berechtigt erwiesen. Auf dem vom Beschwerdeführer abgegebenen Paket war unstrittig seine Adresse vermerkt. Dieselbe Adresse geht auch aus dem im Paket mitgesendeten Lebenslauf des Beschwerdeführers hervor. Beides befand sich zum Zeitpunkt der ZMR-Abfrage im Besitz der Beschwerdegegnerin. Sie konnte somit davon ausgehen, dass der Beschwerdeführer unter dieser Adresse postalisch erreichbar sein wollte. Wenn die Beschwerdegegnerin vorbringt, dass im Zuge der Ermittlungsarbeiten eine weitere Adresse des Beschwerdeführers im PAD ausfindig gemacht werden konnte und deshalb, um eine Zustelladresse zu ermitteln, eine Abfrage im ZMR gem § 16a Abs. 9 MeldeG erforderlich gewesen sei, so ist diesem Vorbringen entgegenzuhalten, dass § 16a Abs. 9 MeldeG explizit darauf abstellt, dass für den der Abfrage zugrunde liegenden Gesetzesvollzug der Hauptwohnsitz eines Menschen maßgeblich ist. Da es der Beschwerdegegnerin vorliegend jedoch nur darauf ankam, eine Zustelladresse (vgl dazu die Legaldefinition des § 2 Z 3 und 4 ZustG, die eben nicht auf das Erfordernis des Hauptwohnsitzes abstellt) zu ermitteln und diese sich eindeutig einerseits aus dem Absendervermerk auf dem Kuvert und andererseits aus dem Lebenslauf des Beschwerdeführers ergab, erwies sich die Abfrage im ZMR als nicht von § 16a Abs. 9 MeldeG gedeckt und somit als unrechtmäßige Beschränkung des Anspruchs auf Geheimhaltung durch eine Behörde gem § 1 Abs. 2 DSG 2000. Selbst wenn man von der Zulässigkeit einer Abfrage im ZMR ausgehen wollte, so erwies sich diese vorliegend – aufgrund des oben Ausgeführten – als nicht notwendig und somit iSd § 1 Abs. 2 in Verbindung mit § 7 Abs. 3 DSG 2000 als nicht gelindestes Mittel. Selbst im Falle einer zulässigen ZMR-Abfrage hätte mit einer einfachen Abfrage gem § 16 Abs. 1 MeldeG betreffend den aktuellen (Haupt-)Wohnsitz des Beschwerdeführers das Auslangen gefunden werden können (vgl dazu den Bescheid der Datenschutzkommission vom 7. Juni 2005, GZ K121.006/0007-DSK/2005). Der Beschwerde war daher in diesem Punkt stattzugeben.

Die Beschwerde erweist sich jedoch als unbegründet, soweit sie die Abfrage im EKIS betrifft. Gem §§ 16, 28a und 53 Abs. 1 Z 3 SPG sind die Sicherheitsbehörden zur Gefahrenerforschung und zur Gefahrenabwehr (ua auch zur Abwehr gefährlicher Angriffe) verpflichtet und dürfen zu diesem Zweck personenbezogene Daten ermitteln und weiterverarbeiten. Die erläuternden Bemerkungen zur SPG-Novelle 2006, BGBl I 158/2005, mit welcher § 53 Abs. 1 Z 3 zuletzt novelliert wurde, führen dazu folgendes aus (1188 dB XXII. GP, 5): »Mit der SPG-Novelle 2000 wurde § 28a Abs. 1 SPG geschaffen, um klarzustellen, dass jeder Gesetzesauftrag zur Gefahrenabwehr implizit stets auch die Teilaufgabe der Gefahrenerforschung umfasst. (Bereits die Stammfassung des SPG enthielt in den Definitionen des § 16 Abs. 4 den Hinweis auf diese Teilaufgabe, allerdings ohne daran spezifische Befugnisse zu knüpfen.) Der Begriff der Gefahrenerforschung des § 28a Abs. 1 ist so zu verstehen, dass die Sicherheitsbehörden bereits bei einem, durch bestimmte Indizien erhärtetem Gefahrenverdacht die Frage zu beantworten haben, ob überhaupt eine Gefahr vorliegt, die sicherheitspolizeiliches Einschreiten erforderlich macht. Es wurde durch die Textierung des § 28a damit außer Streit gestellt, dass im Verdachtsfall Gefahrenerforschung der Gefahrenabwehr vorangehen muss, aber die zur Aufgabenerfüllung notwendige Informationsgewinnung wurde im 4. Teil des SPG nicht verankert. Im Regelfall wird es aber notwendig sein, durch die Erhebung von Informationen (auch personenbezogener Daten) das Vorliegen einer Gefahr zu bestätigen und Aufschluss über die Möglichkeiten ihrer Bekämpfung zu geben, oder festzustellen, dass keine Gefahr gegeben ist und die Aufgabe samt Datenermittlung zu beenden ist. Wenn die Ermächtigung zu Dateneingriffen gemäß § 53 Abs. 1 Z 2a bei der weit im Vorfeld von konkreten Gefahren angesiedelten ‚erweiterten Gefahrenerforschung' des § 21 Abs. 3 zulässig ist, so muss dies umso mehr auch gelten, um einen durch Indizien hinreichend konkretisierten Verdacht auf den Grund zu gehen.

Wenn beispielsweise per Internet vage Drohungen gegen einen ausländischen Staatsbesuch ausgestoßen werden, haben die Sicherheitsbehörden im Wege der Datenermittlung die Gefährdungssituation einzuschätzen.

Ähnlich verhält es sich, wenn etwa ein Fan eine im öffentlichen Leben stehenden Persönlichkeit durch das Schreiben von Briefen und Versuche der Kontaktaufnahme belästigt, und andeutet, bei der nächsten sich bietenden Gelegenheit (etwa anlässlich einer Autogrammstunde) eine ‚Handlung setzen zu wollen, die Aufmerksamkeit erregt', so obliegt es der Exekutive, durch das Sammeln von Informationen über diese Person herauszufinden, ob ein gefährlicher Angriff gegen die Person des öffentlichen Lebens droht und allenfalls durch adäquate Maßnahmen vorzukehren.

Es erfolgt daher in § 53 Abs. 1 in Z 3 eine Klarstellung dahingehend, dass die Verwendung von personenbezogenen Daten in einer Datenanwendung auch für die Gefahrenerforschung gemäß § 28a Abs. 1 zulässig ist.«

Der Beschwerdegegnerin kann aufgrund der auf dem Kuvert sichtbaren Vermerke, der Eigenart des Konvoluts sowie der im Paket bzw. Kuvert befindlichen Dokumente, die – was der Beschwerdeführer nicht bestritten hat – nicht zusammenhängende, teilweise unverständliche Aussagen enthielten, nicht entgegengetreten werden, wenn sie aufgrund dessen zum Zweck der – prioritär durchzuführenden – Gefahrenerforschung eine Abfrage in der Zentralen Informationssammlung gem § 57 SPG zur Person des Beschwerdeführers durchführte, um allenfalls adäquate Vorkehrungsmaßnahmen zur Gefahrenabwehr zu treffen. Für die Verwendung personenbezogener Daten des Beschwerdeführers bestand in diesem Fall eine gesetzliche Ermächtigung, weshalb sich die behördliche Beschränkung des Rechts auf Geheimhaltung als rechtmäßig gem §§ 1 Abs. 2, 7 Abs. 1 und 8 Abs. 1 Z 1 DSG 2000 einerseits aber auch gem §§ 28a Abs. 3 und 53 Abs. 1 Z 3 SPG erwies. Die Beschwerde war daher in diesem Punkt als unbegründet abzuweisen.

p. Verwendung von Daten für Mieterbefragung (K121.906/0003-DSK/2013, 20.2. 2013)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass der Beschwerdegegner (eine Hausverwaltung) unbefugt Hauptmieterdaten einer Wohnhausanlage (Wohnsitz des Beschwerdeführers) an eine Hausbetreuungsgesellschaft weitergegeben habe. Diese habe die Daten (Name und Vorname, Zustelladresse und/oder Anschrift des Mietgegenstandes von Mietern) für Zwecke der Versendung eines Fragebogens (Mieterbefragung) verwendet. Diese Gesellschaft sei im DVR bei den Empfängern »sensibler Daten« nicht erwähnt. Zum behaupteten Recht auf Löschung gab es keine näheren Ausführungen.

Zwischen dem Beschwerdegegner und der Hausbetreuungsgesellschaft besteht wirksam seit September 2011 eine Vertragsbeziehung, die u.a. auch »Erstellung und Versand von Serienbriefen an Mieterinnen und Mieter sowie die Bearbeitung und Aufbereitung von deren schriftlichen Rückmeldungen« umfasst. Im Juli 2011 haben die Parteien außerdem einen allgemeinen datenschutzrechtlichen Dienstleistervertrag abgeschlossen, der gem § 10 Abs. 2 DSG 2000 der Datenschutzkommission vorgelegt und im September 2011 zur Kenntnis genommen worden ist. Im Mai 2012 besorgte die Hausbetreuungsgesellschaft im Rahmen des erstgenannten Vertrags den Versand eines Fragebogens (Gegenstand: zukünftige Gestaltung der Hausbetreuung, Übernahme der Betreuung durch einen »Hausbetreuer neu«) u.a. an die Mieterinnen und Mieter der gegenständlichen Wohnhausanlage. Für diesen Zweck wurden auch die den Beschwerdeführer betreffenden Daten zu den Datenarten »Ordnungsbegriff«, »Titel, Anrede, Vorname, Nachname« und »Anschrift des Mietobjekts« aus der Datenanwendung des Beschwerdegegners ausgewählt und von der Hausbetreuungsgesellschaft für die Adressierung und den Versand des Schreibens verwendet.

Rechtliche Würdigung:

Entscheidend ist die Frage, ob die Datenverwendung für Zwecke einer im Rahmen eines datenschutzrechtlichen Dienstleistungsverhältnisses vorgesehenen Aufgabe erfolgt ist. Seit Inkrafttreten des DSG 2000 umfasst das datenschutzrechtliche Dienstleistungsverhältnis nicht mehr bloß typische IT-Dienstleistungen wie das Speichern von Daten bzw. den Betrieb von Datenverarbeitungsanlagen. Gem § 4 Z 5 DSG 2000 macht jede Datenverwendung für Zwecke eines vom datenschutzrechtlichen Verantwortlichen, dem Auftraggeber, dessen gesetzmäßige Bezeichnung auch so zu erklären ist, »aufgetragenen Werkes« den Vertragspartner zum Dienstleister im datenschutzrechtlichen Sinne.

Grundsätzlich ist das Handeln des Dienstleisters dem Auftraggeber datenschutzrechtlich in allen Fällen zuzurechnen. Einem Betroffenen kommt kein subjektives Recht zu, auf die Auswahl eines Dienstleisters Einfluss zu nehmen oder eine Überlassung seiner Daten zu untersagen bzw. dagegen Widerspruch einzulegen. Folgerichtig liegt beim Datenaustausch im Rahmen eines Dienstleistungsverhältnisses daher keine Übermittlung vor, da sich gem § 4 Z 12 DSG 2000 der Auftraggeber nicht selbst (außer im Spezialfall der »Übermittlung durch Zweckänderung« gem § 4 Z 12 letzter Halbsatz DSG 2000) Daten übermitteln kann. Der Datenaustausch zwischen Auftraggeber und Dienstleister, die Überlassung, allein greift noch nicht in schutzwürdige Geheimhaltungsinteressen des Betroffenen ein. Betreffend eine zweckändernde Datenverwendung liegt hier kein entsprechendes Vorbringen vor, auch im Ermittlungsverfahren hat sich nichts ergeben, das einen solchen Schluss zulassen würde. Es war daher davon auszugehen, dass die Hausbetreuungsgesellschaft im Rahmen ihrer Aufgaben als Dienstleister gehandelt hat. Datenschutzrechtlich liegt daher kein Unterschied zu dem Fall vor, dass der Beschwerdegegner die Mieterdaten selbst für Ausdruck und Adressierung eines an die Betroffenen gerichteten Schreibens verwendet hätte.

Wie der Beschwerdegegner zutreffend geltend gemacht hat, sind hier keine sensible Daten des Beschwerdeführers verwendet worden (vgl § 4 Z 2 DSG 2000). Hinsichtlich der materiellrechtlichen Zulässigkeit des Handelns (Verwendung der Daten für den Versand eines Fragebogens) kann sich dieses auf allgemeine überwiegende Interessen des Beschwerdegegners (§ 8 Abs. 1 Z 4 DSG 2000) im Rahmen des Mietrechtsverhältnisses (rechtliche Befugnis gem § 7 Abs. 1 DSG 2000) stützen. § 47 Abs. 2 Z 1 DSG 2000, auf den sich der Beschwerdegegner stützen möchte, müsste nur herangezogen werden, wenn der ursprüngliche Zweck der Datenverwendung (Angelegenheit des Mietrechts und der Hausverwaltung des städtischen Unternehmens »Wiener Wohnen«) überschritten würde, die Daten also übermittelt worden wären. Dies ist hier aber nicht der Fall.

Es erfolgte daher kein rechtswidriger Eingriff in schutzwürdige Geheimhaltungsinteressen des Beschwerdeführers; die Beschwerde war diesbezüglich abzuweisen.

Da keine Übermittlung erfolgte und nicht in das Geheimhaltungsrecht des Beschwerdeführers eingegriffen wurde, kommt ihm hinsichtlich des Datenempfängers auch kein Löschungsrecht zu. Die Hausbetreuungsgesellschaft kann auch keine Pflicht zur »Löschung auf eigene Initiative« (§ 27 Abs. 1 Z 1 DSG 2000) treffen, da sie die Daten des Beschwerdeführers als Dienstleister nicht unter eigener Verantwortung verwendet. Für den Beschwerdegegner als datenschutzrechtlichen Auftraggeber gibt es hingegen während des aufrechten Mietverhältnisses keinen Grund, Daten wie den Namen und die Adresse des Beschwerdeführers zu löschen.

Darüber hinaus hat der Beschwerdeführer auch keinerlei Löschungsbegehren nachgewiesen (siehe § 31 Abs. 4 DSG 2000) oder auch nur behauptet, was – über das eben Abgehandelte hinaus – Voraussetzung für eine Verletzung des subjektiven Rechts auf Löschung eigener Daten wäre. Die Beschwerde enthält zu dieser Frage auch kein näheres Vorbringen und war daher auch in diesem Punkt abzuweisen.

q. Verwendung von Gesundheitsdaten für Zwecke der Überprüfung der Lenkberechtigung (K121.723/0003-DSK/2013, 30.4. 2013)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass das Büro für Waffen- und Veranstaltungsangelegenheiten bei der Beschwerdegegnerin (einer ehemaligen Bundespolizeidirektion, nunmehr Landespolizeidirektion) im November 2010 dem Verkehrsamt bei der Beschwerdegegnerin gesetzwidrig intern eine Information über den Inhalt eines amtsärztlichen Gutachtens (eingeholt im Ermittlungsverfahren betreffend seine Vorstellung gegen ein durch Mandatsbescheid verhängtes Waffenverbot) übermittelt habe, worauf ein Verfahren zur Überprüfung seiner Lenkberechtigungen eingeleitet worden sei.

Mit Bescheid aus September 2011 hatte die Datenschutzkommission die Beschwerde zunächst unter Berufung von lebenswichtigen Interessen des Betroffenen als Rechtfertigung für die Datenverwendung als unbegründet abgewiesen.

Dagegen hat der Beschwerdeführer erfolgreich Beschwerde an den VfGH erhoben. Mit Erkenntnis vom 11. Oktober 2012, Zl B 1369/11, wurde der Bescheid aufgehoben. Der VfGH führte aus, bei der behördeninternen Weitergabe von Informationen betreffend den Gesundheitszustand des Beschwerdeführers handle es sich um eine Übermittlung – nämlich eine Verwendung von Daten für ein anderes Aufgabengebiet der Beschwerdegegnerin als Auftraggeber – von sensiblen personenbezogenen Daten im Sinne des § 4 Z 2 und Z 12 DSG 2000. Ein entsprechender Eingriff in das verfassungsgesetzlich gewährleistete Geheimhaltungsrecht unter Berufung auf die lebenswichtigen Interessen des Betroffenen dürfe nur dann erfolgen, wenn eine Zustimmung nicht

eingeholt werden könne; dies ergebe sich schon aus § 1 Abs. 2 letzter Satz DSG 2000, wonach zulässige Eingriffe jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden dürfen. Der VfGH schloss sich der Auffassung der Datenschutzkommission, wonach ein Eingriff aus »lebenswichtigem Interesse« auf § 1 Abs. 2 DSG 2000 iVm § 3 Abs. 1 Z 3 iVm § 8 und § 9 sowie iVm § 24 FSG und § 3 Abs. 1 Z 1, § 5 Abs. 1 Z 4 und § 13 FSG-GV gestützt werden könne, nicht an, dienten diese Bestimmungen doch vorrangig dem Schutz (lebenswichtiger) Interessen anderer Verkehrsteilnehmer. Selbst unter Zugrundelegung dieser Ansicht erweise sich die Begründung im angefochtenen Bescheid aber jedenfalls als unzureichend, weil die belangte Behörde nicht geprüft habe, ob im konkreten Fall – etwa aufgrund der Schwere der psychischen Erkrankung oder des Bestehens einer unmittelbaren Gefahr für den Beschwerdeführer – eine Situation vorlag, die einer physisch bedingten Zustimmungsunfähigkeit (etwa im Sinne einer Bewusstlosigkeit) gleichzuhalten ist und deshalb eine Übermittlung von Gesundheitsdaten im lebenswichtigen Interesse des Betroffenen (ohne den Versuch, seine Zustimmung einzuholen) gerechtfertigt war. Dadurch sei der Beschwerdeführer in seinem verfassungsgesetzlich gewährleisteten Recht auf Geheimhaltung gem § 1 Abs. 1 DSG 2000 verletzt worden. Weiters konnte aus dem Erkenntnis des VfGH geschlossen werden, dass allenfalls auch zu prüfen wäre, ob aufgrund des dritten Tatbestandes des § 1 Abs. 2 DSG 2000 (Wahrung überwiegender berechtigter Interessen anderer) ergangene einfachgesetzliche Bestimmungen (möglicherweise § 9 Z 8 DSG 2000) die Datenübermittlung im konkreten Fall – auch aus anderen Gründen als dem lebenswichtigen Interesse des Betroffenen – rechtfertigen könnten.

Dem Beschwerdeführer wurde mit Mandatsbescheid der Beschwerdegegnerin aus Juni 2010 der Besitz von Waffen und Munition verboten. Dagegen hat der Beschwerdeführer Vorstellung erhoben. Im darauf folgenden Ermittlungsverfahren zur Überprüfung etwaiger medizinischer Gründe für die Verhängung des Waffenverbots hat eine Amtsärztin im November 2010 Befund und Gutachten über den Beschwerdeführer erstellt. Die Sachverständige kam zu dem Schluss, dass der Beschwerdeführer an einer Depression leide und der Verdacht auf eine psychische Erkrankung aus dem schizophrenen Formenkreis bestehe. Aggressionen und Gewaltausbrüche seien aktenkundig. Es wurde empfohlen, auch die Eignung zum Lenken von Kraftfahrzeugen einer Überprüfung zu unterziehen.

Nur Letzteres wurde dem Verkehrsamt der Beschwerdegegnerin mit interner Note aus November 2010 mitgeteilt, ohne nähere Angaben zum Gesundheitszustand des Beschwerdeführers zu machen.

Im Jänner 2011 richtete das Verkehrsamt eine interne Note an den Chefärztlichen Dienst, in der die Amtsärztin um Stellungnahme ersucht wurde, welche konkreten Hinweise sich betreffend die Erkrankung des Beschwerdeführers bzw. dessen beschränkte Eignung zum Lenken von Kraftfahrzeugen aus dem amtsärztlichen Gutachten vom November 2010 ergeben würden. Dazu heißt es im Antwortschreiben: »... Es besteht eine Depression und der Verdacht auf eine Erkrankung aus dem schizophrenen Formenkreis. ... lebt in einer Scheinwelt, es kommt immer wieder zu Gewaltdurchbrüchen vor allem im familiären Umfeld. Eine fachärztliche Behandlung wurde beim damaligen Kenntnisstand ... nicht durchgeführt.«

Das Verkehrsamt leitete darauf ein Verfahren zur Entziehung von Lenkberechtigungen wegen fehlender gesundheitlicher Eignung ein und ließ den Beschwerdeführer gem § 24 Abs. 4 FSG zu einer neuerlichen amtsärztlichen Untersuchung laden. Beweisergebnisse, nach denen der Beschwerdeführer im Zeitraum zwischen dem Jänner und Anfang März 2011 an einer schwerwiegenden psychischen Erkrankung gelitten hätte, die seine Einsichts- und Urteilsfähigkeit soweit beeinträchtigt hätte, dass eine einer Bewusstlosigkeit gleichzuhaltende Zustimmungsunfähigkeit gegeben war, lagen nicht vor.

Rechtliche Würdigung:
A. Anwendbarkeit der einfachgesetzlichen Bestimmungen des DSG 2000

Gemäß der vom VfGH im Erkenntnis vom 11. Oktober 2012, Zl B 1369/11, geäußerten Rechtsansicht ist die Beschwerdegegnerin als »Auftraggeber... von sensiblen personenbezogenen Daten iSd § 4 Z 2 und Z 12 DSG 2000« zu behandeln. Der VfGH lässt mehrfach seine Auslegung des Gesetzes erkennen, wonach auch hier der Ablauf der Verwendung von Daten des Beschwerdeführers an allen einfachgesetzlichen Bestimmungen des DSG 2000 zu messen ist, etwa durch den Hinweis auf eine mögliche Anwendbarkeit des § 9 Z 8 DSG 2000. Hier ist davon auszugehen, dass zumindest teilweise ein Ablauf von zielorientierten, logisch verbundenen Verwendungsschritten (vgl die Wortfolge »oder auch nur teilweise« in § 4 Z 7 DSG 2000) vorliegt und daher die §§ 4 ff auch direkt auf die Frage des Eingriffs in das Grundrecht auf Geheimhaltung anzuwenden sind.

B. direkte Anwendung des § 1 Abs. 2 DSG 2000

Der VfGH hat weiters die Rechtsansicht vorgegeben, wonach der erste Halbsatz des § 1 Abs. 2 DSG 2000 mit dem Wortlaut »Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt ...« so zu verstehen ist, dass diese Bestimmung nur dann direkt und ohne Vorliegen einer anderen (einfach-) gesetzlichen Regelung als Grundlage für Eingriffe in das Recht auf Geheimhaltung von Daten herangezogen werden kann, wenn aufgrund der Schwere einer Erkrankung oder sonstigen Beeinträchtigung der Betroffene im Eingriffszeitpunkt nicht in der Lage war, seine eigenen Interessen wahrzunehmen.

Ein solcher Sachverhalt ist hier nicht nachgewiesen.

C. Anwendung des § 9 DSG 2000

Der VfGH hat in seinem Erkenntnis schließlich angemerkt, dass die Datenschutzkommission auch die Anwendbarkeit des § 9 Z 8 DSG 2000 zu prüfen gehabt hätte.

Das ergänzende Ermittlungsverfahren hat bestätigt, dass aus Sicht der Beschwerdegegnerin beim Beschwerdeführer der begründete Verdacht einer schwerwiegenden psychischen Erkrankung, insb einer Erkrankung aus dem schizophrenen Formenkreis vorlag. Das amtsärztliche Gutachten aus März 2011 spricht wörtlich davon, dass der Beschwerdeführer »in einer Scheinwelt« lebe und es »immer wieder zu Gewaltdurchbrüchen« komme.

Daraus durfte die Beschwerdegegnerin den Schluss ziehen, dass der Beschwerdeführer unter einer Beeinträchtigung seiner gesundheitlichen Eignung zum Lenken von Kraftfahrzeugen gem § 5 Abs. 1 Z 4 FSG-GV litt, und die Belassung einer Lenkberechtigung daher gem § 13 Abs. 2 Z 1 oder 4 FSG-GV iVm § 24 FSG nur aufgrund einer die kraftfahrspezifische Leistungsfähigkeit beurteilenden psychiatrischen fachärztlichen Stellungnahme zulässig wäre. Aus dem Inhalt des vorliegenden amtsärztlichen Gutachtens war darüber hinaus für den Einzelfall der Schluss zulässig, dass durch das Verhalten des Beschwerdeführers, insb die Möglichkeit von »Gewaltdurchbrüchen«, eine konkrete Gefährdung anderer Verkehrsteilnehmer zu befürchten war. Diese einschlägigen Bestimmungen des Führerscheingesetzes und der Führerscheingesetz-Gesundheitsverordnung dienen – wie auch der VfGH in seinem Erkenntnis anführt – vorrangig dem Schutz lebenswichtiger Interessen anderer Verkehrsteilnehmer. Da das Lenken von Kraftfahrzeugen eine bereits an sich gefährliche Tätigkeit darstellt, ist durch Verkehrsteilnehmer, bei denen zu befürchten ist, dass hinsichtlich deren psychischer

Verfassung eine Gefahr für andere Verkehrsteilnehmer ausgehe, eine besondere Sorgfalt zu wahren. Ein Verkehrsteilnehmer – der wie oben beschrieben unter einer Erkrankung aus dem schizophrenen Formenkreis leidet – stellt eine hohe Gefahr für Leben und Gesundheit anderer Verkehrsteilnehmer dar.

Aufgrund des vorliegenden Sachverhaltes war jedenfalls die Grundlage dafür gegeben, gem § 9 Z 8 DSG 2000 zur »Wahrung lebenswichtiger Interessen eines anderen«, worunter auch jeder einzelne Verkehrsteilnehmer zu verstehen ist, der dem Beschwerdeführer im Zustand psychischer Beeinträchtigung begegnen könnte, behördenintern das Verkehrsamt – insb weil im Akt betreffend die Verhängung eines Waffenverbotes eine Kopie der Lenkerberechtigung vorlag – über entsprechende Bedenken zu informieren bzw. diese zur Kenntnis zu nehmen.

Die schutzwürdigen Geheimhaltungsinteressen wurden im vorliegenden Fall nicht verletzt.

Die Übermittlung des Inhalts des amtsärztlichen Gutachtens erfolgte in weiterer Folge im Übrigen erst nach einer entsprechenden Anfrage des Verkehrsamts und kann sich daher auch auf § 9 Z 4 DSG 2000, die Bestimmung über die Verwendung sensibler Daten für Zwecke der Amtshilfe, stützen.

Die Beschwerde war daher (erneut) abzuweisen.

r. Ausfolgung von Sicherstellungsprotokollen (K121.909/0010-DSK/2013, 22.5. 2013)

Sachverhalt:
Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung durch Mitteilungen, die Beamte einer Polizeiinspektion A (PI A), deren Handeln der Beschwerdegegnerin als Sicherheitsbehörde zuzurechnen sei, im August 2012 seiner Mutter gemacht hätten.

Die PI A führte im Jahr 2012 unter der Verantwortung der Beschwerdegegnerin als Sicherheitsbehörde erster Instanz ein kriminalpolizeiliches Ermittlungsverfahren gegen den Beschwerdeführer als Beschuldigten wegen des Verdachts von Straftaten wider § 27 Abs. 1 des SMG. Dieses Verfahren wurde mit dem Abschluss-Bericht vom Oktober 2012 (Strafanzeige wegen Verdachts nach § 27 Abs. 1 Z 2 SMG – Anbau der Cannabispflanze) abgeschlossen.

Bereits zuvor, nämlich im Juni 2012, war der Beschwerdeführer im kriminalpolizeilichen Ermittlungsverfahren einer weiteren PI B gegen den Beschuldigten X von ihm sowohl als Käufer wie als Verkäufer von Cannabiskraut bezeichnet worden. Dieses Faktum war kurz darauf bei der PI A amtsbekannt.

An einem näher bezeichneten Tag im August 2012 führten zwei Beamte der PI A aus eigener Macht der Sicherheitsbehörde wegen Gefahr im Verzug im Haus der Familie eine Durchsuchung des vom Beschwerdeführer benutzten Zimmers durch. Diese Durchsuchung folgte dem der PI A angezeigten Fund einer Cannabispflanze in einem Wald in der Nähe des Hauses, mit deren Anbau der Beschwerdeführer in Verbindung gebracht wurde, und der Wahrnehmung von Cannabisblättern auf dem Schreibtisch des Beschwerdeführers durch die – mit Zustimmung der Mutter des Beschwerdeführers – das Zimmer betretenden Beamten. Diese Durchsuchung wurde mit einem Beschluss des zuständigen Landesgerichts nachträglich bewilligt.

Anwesend waren neben dem Beschwerdeführer auch dessen Mutter und dessen Freundin. Beiden wurde dadurch bekannt, dass gegen den Beschwerdeführer wegen Verdachts von Vergehen gegen das SMG ermittelt wurde. Anlässlich dieser Durchsuchung wurden mehrere Gegenstän-

de sichergestellt, darunter Cannabisprodukte sowie Löschblätter, die wegen ihres Aussehens und ihrer Eignung als Trägermaterial für LSD (Aufdruck, Perforierung) im Durchsuchungs- und Sicherstellungsprotokoll als mögliche LSD-Trips bezeichnet wurden.

Am Nachmittag desselben Tages wurde, wie anlässlich der Durchsuchung angekündigt, versucht, dem Beschwerdeführer das Durchsuchungs- und Sicherstellungsprotokoll (Bestätigung gemäß §§ 111 Abs. 4 und 122 Abs. 3 StPO) unverzüglich persönlich auszufolgen. Da er zu diesem Zeitpunkt jedoch abwesend war, wurde die Urkunde an seine Mutter offen (ohne Kuvert) ausgefolgt und von ihr an der vorgesehenen Stelle unterschrieben. Beim Durchlesen des Durchsuchungs- und Sicherstellungsprotokolls fiel ihr das Wort »LSD« auf, und sie suchte kurz danach die PI A auf und erkundigte sich, was in diesem Zusammenhang sichergestellt worden sei. Sie wurde von einer der ermittelten Beamtinnen unter Vorzeigen der sichergestellten Löschblätter darüber informiert, dass man in diesen LSD-Trips vermute, was aber noch durch eine entsprechende Untersuchung zu bestätigen sei.

Rechtliche Würdigung:
A. zur Zuständigkeit der Datenschutzkommission

Wie der VfGH (Erkenntnis vom 21. 12. 2010, VfSlg 19281/2010) ausgesprochen hat, verbietet es Art. 94 B-VG, eine nachprüfende Kontrolle eines Gerichts über faktische Amtshandlungen einer Sicherheitsbehörde im Zuge der Erfüllung von Aufgaben der Kriminalpolizei vorzusehen, wenn diese aus eigener Macht, dh ohne entsprechende Anordnung einer Justizbehörde (Staatsanwaltschaft oder Gericht) gesetzt werden. Die Wortfolge »oder Kriminalpolizei« in § 106 Abs. 1 StPO wurde aufgehoben.

Ein Vorbringen dahin gehend, dass die in Beschwerde gezogenen Amtshandlungen der PI A im August 2012 auf Anordnung einer Justizbehörde (Gericht oder Staatsanwaltschaft) gesetzt worden sind, lag nicht vor und ist auch im Zuge des Ermittlungsverfahrens nicht hervorgekommen. Auf allen zeitlich entsprechenden Aktenstücken, insb auf dem Durchsuchungs- und Sicherstellungsprotokoll, war als verantwortliche Sicherheitsbehörde die Beschwerdegegnerin angeführt.

Die Datenschutzkommission war daher zur Entscheidung der vorliegenden Beschwerde zuständig.

B. in der Sache selbst, Verletzung des Rechts auf Geheimhaltung

Gemäß der Verfassungsbestimmung § 1 Abs. 2 DSG 2000 bedürfen Eingriffe in das Grundrecht auf Geheimhaltung, die durch eine staatliche Behörde vorgenommen werden, einer gesetzlichen Ermächtigung im Sinne des Art. 8 EMRK (vgl VfGH VfSlg 18146/2007).

Jüngste Entscheidungen des VfGH verlangen auch bei nicht-automationsunterstützter Datenverwendung eine entsprechende gesetzliche Ermächtigung, etwa bspw auch für die behördeninterne Übermittlung eines Sachverständigengutachtens (Verwendung für ein anderes Aufgabengebiet einer Behörde):

»Bei der behördeninternen Weitergabe von Informationen betreffend den Gesundheitszustand des Beschwerdeführers handelt es sich um eine Übermittlung – nämlich eine Verwendung von Daten für ein anderes Aufgabengebiet der BPD Wien als Auftraggeber – von sensiblen personenbezogenen Daten iSd § 4 Z 2 und Z 12 DSG 2000. Da im vorliegenden Fall (unbestrittenermaßen) ein schutzwürdiges Interesse des Beschwerdeführers an der Geheimhaltung dieser Daten besteht, greift ihre Übermittlung in das verfassungsgesetzlich gewährleistete Recht auf Geheimhaltung seiner personenbezogenen Daten gemäß § 1 Abs. 1 DSG 2000 ein.

Ein Eingriff in das verfassungsgesetzlich gewährleistete Geheimhaltungsrecht gemäß § 1 Abs. 2 erster Satz DSG 2000 unter Berufung auf die lebenswichtigen Interessen des Betroffenen darf nur dann erfolgen, wenn eine Zustimmung nicht eingeholt werden kann; dies ergibt sich schon aus § 1 Abs. 2 letzter Satz DSG 2000, wonach zulässige Eingriffe jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden dürfen.« (VfGH, Erkenntnis vom 11. 10. 2012, B 1369/11, Rechtssatz)

Nach der Rechtsprechung der Datenschutzkommission kann ein Eingriff in das (Grund-) Recht auf Geheimhaltung von Daten in nahezu jeder Form erfolgen, darunter auch durch mündliche Übermittlung (vgl Bescheide der Datenschutzkommission vom 31. 8. 2000, GZ: 120.532/22-DSK/00, sowie vom 29. 11. 2005, GZ: K121.050/0015-DSK/2005). Die mündliche oder schriftliche Bekanntgabe, dass gegen eine bestimmte Person kriminalpolizeiliche Ermittlungen geführt werden, ist, ebenso wie die Bekanntgabe von einzelnen, detaillierten Fakten (z. B. Erläuterungen zu sichergestellten Gegenständen), daher eine für das Recht auf Geheimhaltung dieses Betroffenen relevante Datenübermittlung.

Gemäß den Sachverhaltsfeststellungen muss der Eingriff in zwei Teile geteilt betrachtet werden.

- Vornahme der Durchsuchung

Hinsichtlich des gegen den Beschwerdeführer bestehenden Verdachts, Cannabisprodukte besessen bzw. die Cannabispflanze angebaut zu haben, ergibt sich das entsprechende Wissen der Mutter des Beschwerdeführers schon daraus, dass diese mit Zustimmung des Beschwerdeführers bei der Durchsuchung seines Zimmers anwesend war und dadurch vom Anlass und Grund der Durchsuchung (Verdacht des Verkaufs von Cannabiskraut, Entdeckung einer Cannabispflanze, Wahrnehmung von Cannabisblättern im Zimmer des Beschwerdeführers durch die Beamten) und den gefundenen Beweisgegenständen Kenntnis erlangte.

Ein gelinderes Mittel gemäß § 7 Abs. 3 DSG 2000 wurde vom Beschwerdeführer nicht aufgezeigt und hätte wohl nur darin bestehen können, der Mutter entweder während der Durchsuchung überhaupt oder doch vor jeder mündlichen Äußerung der Beamten zur bestehenden Verdachtslage aus dem Raum zu weisen, was wiederum im Widerspruch zur Zustimmung des Beschwerdeführers zur Anwesenheit seiner Mutter gestanden hätte und damit ein Handeln gegen dessen eigene Willensäußerung bedeutet hätte.

Die Mutter durfte daher vom Bestehen eines kriminalpolizeilichen Verdachts hinsichtlich des Besitzes von Cannabisprodukten bzw. des Anbaus der Cannabispflanze erfahren.

- Ausfolgung des Durchsuchungs- und Sicherstellungsprotokolls

Hinsichtlich des durch den Fund der Löschblätter entstandenen oder verstärkten Verdachts betreffend LSD hat sich ergeben, dass dieser Verdacht der Mutter des Beschwerdeführers erst aus der Bestätigung über die vorgenommene Durchsuchung und Sicherstellung (gemäß §§ 111 Abs. 4 und 122 Abs. 3 StPO) bekannt wurde.

In diesem Zusammenhang war zu bemängeln, dass hier ein für den Beschwerdeführer als Adressaten (Betroffener gemäß §§ 111 Abs. 4 und 122 Abs. 3 StPO) bestimmtes Dokument übermittelt wurde, ohne den Inhalt gegen Kenntnisnahme durch Unbefugte während des Vorgangs zu sichern. Für den Fall einer behördlichen Zustellung nach den Bestimmungen des ZustG setzt dieses implizit voraus, dass physische Zustellstücke während des Beförderungsvorgangs verschlossen (in einem Kuvert) aufbewahrt werden, und erst der gemäß § 2 Z 1

ZustG bezeichnete Empfänger oder ein gesetzlich zulässiger Ersatzempfänger nach Vornahme der Zustellung die Entscheidung treffen kann, ob er das Zustellstück (in der Regel wohl ein Kuvert) öffnet bzw. öffnen darf.

Die Datenschutzkommission übersieht nicht, dass die Gestaltung der entsprechenden im Behördengebrauch der Bundespolizei offenbar üblichen Vorlage hier eine offene »Ausfolgung« vorsieht, wobei das Gesetz (wiederum §§ 111 Abs. 4 und 122 Abs. 3 StPO) dies offenkundig als Alternative zur Zustellung betrachtet (arg »auszufolgen oder zuzustellen«). Die Gestaltung eines Formulars kann jedoch keinesfalls über die Vornahme eines Grundrechtseingriffs entscheiden. Die Datenschutzkommission geht in verfassungskonformer Auslegung der Bestimmungen der StPO davon aus, dass hier aufgrund der Regel, stets das gelindere Mittel heranzuziehen (§ 1 Abs. 2 letzter Satz, § 7 Abs. 3 DSG 2000), die Zustellung im Kuvert das zwingend gebotene Mittel der Wahl gewesen wäre. Eine unverschlossene Ausfolgung hätte nur im Fall einer direkten Übergabe an den Beschwerdeführer als Betroffenen erfolgen dürfen. Die Zustellung kann dabei mithilfe der für die nachweisliche Zustellung behördlicher Dokumente vorgesehenen Mittel (Zustellnachweisen) dokumentiert werden.

Die weiteren Vorgänge (Nachfrage der Mutter, Information betreffend die Bedeutung des Begriffs »LSD« im Kontext des Durchsuchungs- und Sicherstellungsprotokolls) waren keine neue Datenübermittlung sondern nur eine unvermeidliche Folge der ersten, unzulässigen Datenübermittlung durch Ausfolgung des Dokuments.

Der Beschwerde war daher in diesem Punkt stattzugeben, darüber hinaus aber abzuweisen.

s. Fehlender Personenbezug bei Befischungsdaten (K121.946/0014-DSK/2013, 14.6.2013)

Sachverhalt:
Die Beschwerdeführerin behauptet eine Verletzung im Recht auf Geheimhaltung personenbezogener Daten dadurch, dass das Amt einer Landesregierung (Beschwerdegegner) Befischungsdaten zu ihrem Fischereirecht an Sachverständige zwecks Erstellung von Privatgutachten im Zuge der Planung eines Kraftwerks weitergegeben worden seien.

Die Beschwerdeführerin ist Fischereiberechtigte im verfahrensgegenständlichen Fließgewässer zwischen zwei näher bezeichneten Punkten. Eine näher bezeichnete Messstelle befindet sich im Fischereirevier der Beschwerdeführerin.

Im Oktober 2011 wurde bei dieser Messstelle auf Basis der Gewässerzustandsüberwachungsverordnung (GZÜV) eine Elektrobefischung durchgeführt.

Der Beschwerdegegner übermittelte den Messbericht dazu aufgrund eines Ersuchens vom März 2012 an die Projektanten eines Kraftwerksprojekts zur projektbezogenen Verwendung.

Die im Rahmen der Elektrobefischung befischte Länge deckt sich nicht mit der Länge des Fischereireviers der Beschwerdeführerin.

Bei der gegenständlichen Messstelle handelt es sich um eine Messstelle der operativen Überwachung gemäß § 10 GZÜV.

Rechtliche Würdigung:
Grundvoraussetzung für eine Verletzung im Recht auf Geheimhaltung ist das Vorliegen personenbezogener Daten. Dies wäre vorliegend jedoch nur möglich, wenn aufgrund der GZÜV-

Messung (gesicherte) Rückschlüsse auf den Fischbestand im Fischereirevier der Beschwerdeführerin, und somit auf die Beschwerdeführerin selbst, gezogen werden könnten. Dies war jedoch nicht der Fall.

Die §§ 59c-59f WRG 1959 regeln die Erhebung des Zustandes von Gewässern. Auf Basis dieser Bestimmungen wurde die GZÜV erlassen. Bei der gegenständlichen Messstelle handelt es sich um eine Messstelle der operativen Überwachung gemäß § 10 GZÜV. Ziel der operativen Überwachung gemäß § 59f WRG 1959 ist die Feststellung des Zustandes von Oberflächenwasserkörpern und Grundwasserkörpern.

Dazu bestimmt § 10 Abs. 2 GZÜV, welcher insoweit § 59 f Abs. 2 WRG 1959 konkretisiert, dass Messstellen so zu errichten sind, dass sie im Hinblick auf die Belastung des Wasserkörpers repräsentativ für die Bestimmung des Zustandes sind. Nach § 11 Abs. 1 GZÜV hat die operative Überwachung jene Parameter zu umfassen, die für die Belastung des Wasserkörpers kennzeichnend sind. Diese Parameter sind für jede Belastung in Anlage 8 festgelegt. Anlage 8 nennt als Parameter u. a. Fische (ohne diesbezüglich jedoch zwischen einzelnen Arten zu differenzieren).

Daraus folgt einerseits, dass die Festlegung der Messstellen unabhängig von den Grenzen der Fischereireviere erfolgt. Der Standort einer Messstelle wird nämlich dadurch bestimmt, dass die von ihr gemessenen Werte repräsentativ für die Bestimmung des Zustandes des Wasserkörpers (und zwar nicht bloß eingeschränkt auf ein bestimmtes Fischereirevier) sind. Es ist daher möglich, dass in einem Fischereirevier mehrere Messstellen vorhanden sind oder auch gar keine. Folglich legt § 72 Abs. 1 lit g WRG 1959 für die Vornahme von Messungen eine Duldungsverpflichtung u. a. für Fischereiberechtigte fest.

Weiters folgt daraus, dass eine auf Basis von §§ 10 und 11 GZÜV durchgeführte Messung nicht darauf abzielt, den exakten Fischbestand im Messbereich einer Messstelle zu erheben. Zwar wird auch – wie aus dem vom Beschwerdegegner vorgelegten Messbericht hervorgeht – erhoben, welche Fischarten (bspw Bachforelle, Koppe) im (räumlich begrenzten) Messbereich vorkommen und wie viele Fische – wiederum differenziert nach Arten – während der Messdauer gefangen wurden. Jedoch dient diese Erhebung – wie sich aus Anlage 8 zur GZÜV eindeutig ergibt – nicht der exakten Bestimmung des Fischbestandes. Die Fischdaten sind lediglich einer von mehreren Parametern zur Bestimmung der Belastung des Wasserkörpers. Es handelt sich dabei um Momentaufnahmen an Messstellen, die zur Messung der Qualität des Gewässers notwendig sind.

Folglich kann eine Messung auch nicht dazu dienen, den (exakten) Fischbestand eines Fischereireviers zu bestimmen.

Es lassen sich daher aus dem vom Beschwerdegegner an die Projektanten übermittelten Bericht vom Oktober 2011 keine Rückschlüsse auf den Fischbestand im Fischereirevier der Beschwerdeführerin – und damit auf das Verhalten der Beschwerdeführerin als Fischereiberechtigte – ziehen. Auch aus dem Bericht vom Oktober 2011 selbst ergibt sich eindeutig, dass der Fischbestand die »morphologischen Gegebenheiten« widerspiegelt. Dass der Fischbestand mit Fischereimaßnahmen der Beschwerdeführerin zusammenhängt, geht aus dem Bericht hingegen nicht hervor.

Es liegen im konkreten Fall somit keine personenbezogenen Daten im Sinne des § 4 Z 1 DSG 2000 vor, weshalb die Beschwerdeführerin durch die Übermittlung des Berichts auch nicht in ihrem Recht auf Geheimhaltung verletzt sein kann.

t. Lichtbild im kriminalpolizeilichen Ermittlungsverfahren (K121.956/0009-DSK/2013, 26.6. 2013)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung personenbezogener Daten dadurch, dass eine Bezirkshauptmannschaft als Sicherheitsbehörde (Beschwerdegegnerin) ohne Rechtsgrundlage und gegen seinen Willen im Zuge einer polizeilichen Anhörung durch eine Polizeiinspektion (PI) ein Lichtbild angefertigt hätte.

Die PI führte im Frühjahr 2013 ein kriminalpolizeiliches Ermittlungsverfahren gegen den Beschwerdeführer wegen des Verdachts der Übertretung des Suchtmittelgesetzes durch. Im Zuge dessen wurde er mit Ladung zur Vernehmung als Beschuldigter in Bezug auf seine Suchtmittelaktivitäten für Februar 2013 in die PI geladen.

Er wurde vom vernehmenden Polizeibeamten aufgefordert, sich einem Urintest und einer erkennungsdienstlichen Behandlung zu unterziehen, was der Beschwerdeführer verweigerte. Nach Abschluss der Vernehmung fertigte der einvernehmende Beamte gegen den Willen des Beschwerdeführers ein Lichtbild (Frontalansicht) von ihm an und speicherte dieses vorübergehend auf seinem Arbeitsplatz, um es in Folge potenziellen Tatzeugen zu zeigen. Das Lichtbild wurde in einer Zeugenvernehmung verwendet und dort der Beschwerdeführer eindeutig erkannt.

Die PI übermittelte im Februar 2013 einen Bericht an die Beschwerdegegnerin, wonach der Beschwerdeführer die Durchführung einer erkennungsdienstlichen Behandlung verweigert hatte und ersuchte sie, ihm gemäß § 77 Abs. 2 und 3 SPG mit Bescheid die Verpflichtung zur Mitwirkungen an der erkennungsdienstlichen Behandlung für einen Termin im März 2013 aufzuerlegen.

Die PI erstattete weiters im März 2013 einen Abschlussbericht gemäß § 100 Abs. 2 Z 4 StPO an die zuständige Staatsanwaltschaft, welchem u. a. die Vernehmungsprotokolle des Beschwerdeführers sowie des Zeugen beigeschlossen waren, wobei der Beschwerdeführer verschiedener Suchtmittelaktivitäten – u. a. der Weitergabe von Suchtmittel an andere – beschuldigt wurde. Hingewiesen wurde auch darauf, dass der Beschwerdeführer nicht geständig sei und die Durchführung eines Urintests und einer erkennungsdienstlichen Behandlung verweigert habe.

Rechtliche Würdigung:

A. zur Zuständigkeit der Datenschutzkommission

§ 90 SPG sieht eine Zuständigkeit der Datenschutzkommission in Angelegenheiten der Sicherheitsverwaltung vor. Wie festgestellt, wurden gegen den Beschwerdeführer kriminalpolizeiliche Ermittlungen durchgeführt, was gemäß § 22 Abs. 3 SPG zur grundsätzlichen Unanwendbarkeit des SPG – und damit zur Unzuständigkeit der Datenschutzkommission – führen würde.

Nach den Erläuterungen im Bericht des Ausschusses für innere Angelegenheiten (AB 240 dB XVIII. GP S. 3) ist es geradezu typisch, dass Menschen, die in den Verdacht einer gerichtlich strafbaren Handlung geraten sind, nach den in den Bestimmungen des SPG über den Erkennungsdienst festgelegten Regeln behandelt werden. Für sie gilt somit insoweit (neben der StPO) das SPG. Im Sinne des § 22 Abs. 3 SPG endet eine bis zur Klärung der Tat mögliche parallele Anwendbarkeit des SPG neben der StPO mit der Klärung der Identität des Verdächtigen. Ab diesem Zeitpunkt gelten ausschließlich die Bestimmungen der StPO (vgl dazu das Erkenntnis des VwGH vom 16. 2. 2000, Zl. 99/01/0339).

Darüber hinaus ergibt sich aus der Rechtsprechung der Gerichtshöfe des öffentlichen Rechts, dass auch im Zuge eines kriminalpolizeilichen Ermittlungsverfahrens von Organen der Si-

cherheitspolizei durchgeführte Maßnahmen als Maßnahmen der Sicherheitspolizei anzusehen sind, wenn ein direkter Auftrag der Staatsanwaltschaft oder eines Gerichtes an die Organe der Sicherheitspolizei nicht vorliegt und ein Bezug zum Vollzugsbereich des SPG gegeben ist (vgl dazu bspw die Erkenntnisse des VwGH vom 16. 2. 2000, Zl. 95/01/0595, und vom 24. 3. 2004, Zl. 98/12/0515, sowie das Erkenntnis des VfGH vom 21. 12. 2010, VfSlg 19.281).

Ein Vorbringen dahin gehend, dass die in Beschwerde gezogenen Amtshandlungen der PI im Februar 2013 auf Anordnung einer Justizbehörde (Gericht oder Staatsanwaltschaft) gesetzt worden sind, liegt nicht vor, und ist auch im Zuge des Ermittlungsverfahrens nicht hervorgekommen. Auf allen zeitlich entsprechenden Aktenstücken ist als verantwortliche Sicherheitsbehörde die Beschwerdegegnerin angeführt. Weiters ergibt sich aus dem – unbestrittenen – Vorbringen der Beschwerdegegnerin, dass gegen den Beschwerdeführer der Verdacht vorlag, er hätte Suchtmittel auch an andere weitergegeben und dass er nicht geständig sei, sodass der Bezug zur Abwehr eines (weiteren) gefährlichen Angriffs gemäß § 16 Abs. 2 Z 4 iVm § 22 Abs. 3 SPG und damit zum Vollzugsbereich des SPG gegeben war (vgl zur erfahrungsgemäß hohen Wiederholungsgefahr bei Sichtmitteldelikten auch das Erkenntnis des VwGH vom 15. 12. 2005, Zl. 2005/18/0653).

Die Datenschutzkommission war daher zur Entscheidung der vorliegenden Beschwerde zuständig.

B. in der Sache selbst

Gemäß der Verfassungsbestimmung des § 1 Abs. 2 DSG 2000 sind behördliche Beschränkungen des Anspruchs auf Geheimhaltung nur aufgrund einer gesetzlichen Ermächtigung zulässig. Das Anfertigen eines Lichtbildes einer Person stellt unzweifelhaft eine erkennungsdienstliche Maßnahme dar, wie sich aus § 64 Abs. 2 SPG ergibt. § 65 Abs. 1 SPG ermächtigt die Sicherheitsbehörden auch, einen Verdächtigen einer erkennungsdienstlichen Behandlung zu unterziehen. Folglich bestimmt § 65 Abs. 4 SPG, dass der, der erkennungsdienstlich zu behandeln ist, an den erforderlichen Handlungen mitzuwirken hat. § 65 Abs. 5 SPG wiederum legt den Sicherheitsbehörden bestimmte Informationspflichten gegenüber jedem, der erkennungsdienstlich behandelt wird, auf. Weigert sich ein Mensch, sich einer erkennungsdienstlichen Behandlung trotz Aufforderung zu unterziehen, so kann die Sicherheitsbehörde ihm diese Verpflichtung gemäß § 77 Abs. 2 SPG bescheidmäßig auferlegen. Daten, die in Übereinstimmung mit § 65 Abs. 1 SPG ermittelt wurden, können auch an Tatzeugen übermittelt werden, sofern anzunehmen ist, sie würden anhand der Daten zur Identifikation des Täters beitragen (§ 71 Abs. 3 Z 3 SPG).

Im vorliegenden Fall wurde der Beschwerdeführer formlos aufgefordert, sich einer erkennungsdienstlichen Behandlung zu unterziehen, was dieser verweigerte. Folglich wurde die Beschwerdegegnerin von der PI ersucht, dem Beschwerdeführer die Verpflichtung zur Durchführung einer erkennungsdienstlichen Behandlung gemäß § 77 Abs. 2 SPG bescheidmäßig aufzuerlegen. Statt die bescheidmäßige Anordnung abzuwarten, wurde jedoch von dem die Vernehmung durchführenden Beamten ein Lichtbild des Beschwerdeführers angefertigt, mit der Absicht, dieses jenen Tatzeugen zu zeigen, die nach Ausweis der Akten teilweise ebenfalls am gleichen Tag einvernommen wurden, um so die Identifikation des Beschwerdeführers sicherzustellen. Da der handelnde Beamte im Vollzugsbereich des SPG tätig wurde, ist dessen Verhalten der Beschwerdegegnerin zuzurechnen.

Dadurch, dass der die Vernehmung durchführende Beamte den Beschwerdeführer somit trotz dessen Weigerung einer erkennungsdienstlichen Behandlung unterzog, obwohl die hiefür nor-

mierten gesetzlichen Voraussetzungen nicht vorlagen, hat die Beschwerdegegnerin den Beschwerdeführer in seinem Recht auf Geheimhaltung der ihn betreffenden personenbezogenen Daten verletzt.

u. Internet-Lernplattform für Notengebung (K121.933/0029-DSK/2013, 9.8. 2013)

Sachverhalt:

Die Beschwerdeführerin, eine Lehrerin, behauptet eine Verletzung im Recht auf Geheimhaltung eigener Daten (sowie betreffend die Daten ihrer Schülerinnen und Schüler) dadurch, dass der Direktor ihrer Schule vehement die Einführung und verpflichtende Teilnahme an einer Internetanwendung/Lernplattform im Unterricht an der Erstbeschwerdegegnerin (der Schule) betrieben habe. Sie selbst unterrichte dort die Fächer Deutsch und Englisch. Sie habe ihren Vorgesetzten mehrfach u. a. auf die datenschutzrechtliche Problematik des Systems hingewiesen. Im Zuge einer mittlerweile sehr intensiven dienstrechtlichen Auseinandersetzung zwischen ihr und ihrem Vorgesetzten sowie dem Zweitbeschwerdegegner (der Landesschulrat) als Schul- und Dienstbehörde sei sie durch schriftliche Weisung und anschließende Einleitung eines Disziplinarverfahrens wegen zunächst verweigerter Beachtung dieser Weisung schließlich gezwungen worden, sich selbst auf der Plattform zu registrieren, ihre Daten dort zu speichern sowie Daten zur Benotung der schulischen Leistungen ihrer minderjährigen Schülerinnen und Schüler zu verarbeiten. Die Lernplattform sei grundsätzlich für jeden Internetnutzer offen, der sich dort registrieren und auf diesem Weg etwa Namen, Daten zur Schule und teilweise auch Bilder und (E-Mail-) Adressen von Lehrern und Schülern verschaffen könne. Sie widerspreche einigen Regelungen und Vorgaben des DSG 2000 und sei möglicherweise auch im Sinne des § 51 DSG 2000 strafrechtlich relevant. Es sei praktisch der Regelfall, dass Lehrer ohne Rücksprache mit den Schülern deren Daten auf der Plattform registrieren würden, dies überdies auch ohne Einholung der Zustimmung der Eltern, was bei Minderjährigen geboten sei. Weder die Erstbeschwerdegegnerin noch der Zweitbeschwerdegegner hätten die Plattform als Datenanwendung beim Datenverarbeitungsregister gemeldet. Für deren Verwendung im Unterrichtsbetrieb und zur Notengebung fehle es an einer gesetzlichen Grundlage. Die Beschwerdeführerin könne auch nicht ausschließen, sich durch die inzwischen erfolgte Befolgung der Weisung zur Nutzung der Plattform einer Verwaltungsübertretung strafbar gemacht zu haben. Die Beschwerdeführerin beantragte, die erfolgten Rechtsverletzungen, insb des Rechts auf Geheimhaltung festzustellen.

Ein Unternehmen aus Wien betreibt als technischer Dienstleister, gemeinsam mit drei weiteren beteiligten Organisationen (»Projektträger«), darunter das Bundesministerium für Unterricht, Kunst und Kultur (BMUKK) eine Lernplattform im Internet, die besonders auf die Bedürfnisse des Schulbetriebs zugeschnitten worden ist. Das System ermöglicht es u. a. Lehrern (an mittleren und höheren Schulen), ihren Unterricht in Form von Online-Kursen klassenweise zu begleiten, Lernmaterialien (z. B. Hausübungen) zu verteilen und detaillierte Aufzeichnungen über Schularbeits-, Mitarbeits- und Gesamtnoten sowie eine Notenstatistik (für ganze Kurse/Klassen) zu führen. Weiters können über eine Kalenderfunktion private und öffentliche Kalender geführt und Termine bekannt gegeben werden.

Die Datenübertragung zwischen den einzelnen Userinnen und Usern (Lehrer, Schüler und Systemadministratoren) und den eingesetzten Datenverarbeitungsgeräten (PCs und Servern) erfolgt über öffentlich zugängliche Netze mithilfe des verschlüsselten Übertragungsprotokolls https (Hypertext Transmission Protocol Secure).

Zur Registrierung als User genügt die Angabe eines frei wählbaren Usernamens und einer E-Mail-Adresse. Dies ermöglicht die Anlage eines Userprofils, das grundsätzlich allgemein zugänglich ist, dessen Sichtbarkeit (Online-Status, Lesbarkeit der E-Mail-Adresse) aber durch vom User vorzunehmende Privatsphäre-Einstellungen beschränkt werden kann. Es

ist bei Anlage eines Userprofils auch möglich, sich selbst einer bestimmten Schule (etwa der Erstbeschwerdegegnerin) zuzuordnen.

Grundsätzlich steht das System für jedermann zur Registrierung offen. Um als Schüler einer bestimmten Schule Zugang zu einem Kurs/einer Klasse zu erhalten, muss der User von einem mit entsprechenden Berechtigungen (Zuordnung zur Usergruppe Lehrer) versehenen Lehrer in den Kurs/die Klasse aufgenommen werden.

Die Aufzeichnung der Leistung von Schülern erfolgt dergestalt, dass Prüfungsnoten eingetragen und Punkte (etwa für die Mitarbeit in einer bestimmten Zeitperiode) vergeben werden, aus denen das System aufgrund einer Gewichtung eine Gesamtnote errechnet und ausweist. Jeder Schüler kann und darf nur die ihn betreffenden Aufzeichnungen des Lehrers einsehen, jeder Lehrer kann nur die von ihm selbst gemachten Aufzeichnungen sehen, Personen mit weiterreichenden technischen Befugnissen (Administratoren) können auch die Daten ganzer Usergruppen (etwa Lehrern und Schülern einer Schule) einsehen.

An der Erstbeschwerdegegnerin haben sich der Schulleiter, die Schulkonferenz (des Lehrpersonals) und der Schulgemeinschaftsausschuss (Lehrer, Eltern und Schüler) für die Nutzung der Plattform ausgesprochen. Die Beschwerdeführerin war dagegen und verweigerte zunächst die Nutzung. Im Zuge des Jahres 2012 erhielt die Beschwerdeführerin vom Schulleiter jeweils die schriftliche Weisung, die Noten der Schüler/innen auf der Lernplattform zu erfassen und diesen zugänglich zu machen. Die Beschwerdeführerin kam den ersten Weisungen nicht nach, worauf gegen sie ein Disziplinarverfahren eingeleitet wurde. Der Landesschulrat erließ im Oktober 2012 eine Disziplinarverfügung gegen die Beschwerdeführerin, in der wegen Missachtung von Dienstpflichten eine Geldbuße in Höhe von 500 € verhängt wurde. Erst danach hat die Beschwerdeführerin begonnen, ihr bereits im Juni 2011 angelegtes Userprofil zu benutzen, Kurse anzulegen und ihre Schüler betreffende Aufzeichnungen mithilfe der Plattform zu führen.

Betreffend die Beschwerdeführerin konnte die Speicherung folgender Daten festgestellt werden: Vorname, Nachname, E-Mail, Geburtsdatum, User-ID, Registrierungsdatum, Registrierungs-IP, Letzter Besuch, Mitgliedstatus. Dazu kommen Daten zu Mitgliedschaften bzw. Einrichtung in bzw. von 19 Kursen bzw. Klassen (tw. auch in mehrere Gruppen geteilte Schulklassen), in denen die Beschwerdeführerin Aufzeichnungen zur Leistungsbeurteilung vorgenommen hat.

Die Lernplattform ist der Datenschutzkommission nicht als Datenanwendung gemäß §§ 17 ff DSG 2000 gemeldet worden.

Folgende Daten der Beschwerdeführerin sind in einer Liste der Lehrerinnen und Lehrer auf der Homepage der Erstbeschwerdegegnerin öffentlich zugänglich: Name, E-Mail-Adresse, Unterrichtsfächer, Lichtbild.

Rechtliche Würdigung:
A. Reichweite der Entscheidung der Datenschutzkommission

Das Beschwerdeverfahren gemäß § 31 DSG 2000 dient der Wahrung subjektiver Rechte, im vorliegenden Fall der Überprüfung der Frage, ob die Beschwerdeführerin in ihrem Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten verletzt worden ist. Die Beschwerdeführerin war nicht aktiv legitimiert, die Rechte anderer von der Datenverwendung in bzw. auf der Lernplattform Betroffener (insb Kolleginnen oder Kollegen aus der Lehrerschaft der HAK-HAS Feldkirchen bzw. dort eingeschriebene Schülerinnen und Schüler) zu vertreten bzw. deren Rechte geltend zu machen.

Eine derartige »Popularklage« (Klage, die von jemanden erhoben wird, der nicht allein davon betroffen ist) vor der Datenschutzkommission ist nach geltender Rechtslage nicht zulässig und ihre Behandlung daher nicht möglich, da Rechtsverletzungen behauptende Anbringen an die Datenschutzkommission – sowohl die weniger formellen Eingaben gemäß § 30 Abs. 1 DSG 2000 als auch die formellen Beschwerden nach § 31 Abs. 1 und 2 DSG 2000 – nur von Personen gemacht werden können, die behaupten, in ihrer Rechtssphäre von den Handlungen eines datenschutzrechtlichen Auftraggebers betroffen zu sein (Bescheid der Datenschutzkommission vom 30. März 2012, K121.765/0008-DSK/2012).

Das Verfahren war weiters auf die aus dem Grundrecht auf Datenschutz gemäß § 1 DSG 2000 ableitbaren subjektiven Rechte (auf Geheimhaltung, Löschung und Richtigstellung personenbezogener Daten bzw. auf Auskunft über solche Daten) zu beschränken. Auf die Einhaltung von sonstigen Pflichten, die das Gesetz einem datenschutzrechtlichen Auftraggeber auferlegt, besteht kein im Beschwerdeverfahren nach § 31 DSG 2000 durchsetzbarer Anspruch des einzelnen Betroffenen (dies betrifft u. a. die Beachtung der durch § 14 DSG 2000 gebotenen Datensicherheitsmaßnahmen, vgl etwa den Bescheid der Datenschutzkommission vom 2. August 2005, K121.038/0006-DSK/2005).

Auf das Vorbringen der Beschwerdeführerin, soweit es allgemein rechtswidriges Handeln der Beschwerdegegner und Eingriffe in Rechte Dritter behauptet, war daher nur insoweit einzugehen, als aus den Sachverhaltsfeststellungen ableitbar ist, dass Daten der Beschwerdeführerin entgegen gesetzlichen Bestimmungen verwendet worden sind.

B. Lehrerberuf als Ausübung einer öffentlichen Funktion

Die Leistungsbeurteilung gemäß § 18 SchUG ist, jedenfalls gilt dies zweifelsfrei für öffentliche Schulen wie die als Bundesschule eingerichtete Erstbeschwerdegegnerin, durch Gesetz geregeltes staatliches, hoheitliches Verwaltungshandeln, an das sich Rechtsfolgen knüpfen, etwa der Aufstieg in eine höhere Schulstufe oder die Ausstellung eines Zeugnisses (z. B. nach dem Bestehen der Reifeprüfung), das zum Nachweis schulischer Leistungen im Berufsleben dient oder Voraussetzung der Zulassung zu weiteren Bildungslaufbahnen (wie Universitätsstudien) ist. Gegen zahlreiche Entscheidungen der Schulorgane und der Schulbehörden hat die Schülerin oder der Schüler eine Rechtsmittelbefugnis (vgl § 71 Abs. 2 SchUG), die auch eine Überprüfung der Gesetzmäßigkeit der Leistungsbeurteilung umfassen kann (vgl etwa die Ausführungen des VwGH zur Leistungsbeurteilung im Erkenntnis vom 9. März1981, Zl. 3420/80, VwSlg 10391 A/1981).

Gemäß § 18 Abs. 1 SchUG erfolgt die Leistungsbeurteilung durch den Lehrer.

Die Ausübung ihres Berufs als Lehrerin durch die Beschwerdeführerin ist daher die Ausübung einer »öffentlichen Funktion« gemäß § 8 Abs. 3 Z 6 DSG 2000. Sie handelt dabei in Fragen der Leistungsbeurteilung als Organ der Schulbehörde.

Anders als im Fall der Schülerevidenz gemäß § 3 BildDokG (vgl den Bescheid der Datenschutzkommission vom 11. März 2005, GZ: K120.991/0006-DSK/2005 u. a. m.) ist für hoheitliches Verwaltungshandeln im Schulbetrieb datenschutzrechtlich die der Schule übergeordnete Schulbehörde auftraggeberisch verantwortlich. Gemäß § 3 Abs. 1 Z 1 lit. b Bundes-Schulaufsichtsgesetz ist dies der jeweilige Landesschulrat, hier der Zweitbeschwerdegegner. Die Schulbehörde verfügt auch über die gesetzliche Zuständigkeit gemäß § 7 Abs. 1 DSG 2000, Daten betreffend die gesetzlich vorgesehene schulische Leistungsbeurteilung zu verarbeiten.

Daraus folgt, dass weder die Erstbeschwerdegegnerin noch der do. Schulleiter datenschutzrechtlich für die Plattform verantwortlich ist, mag ihr Einsatz auch auf Betreiben des Schulleiters »beschlossen« worden sein. Bereits daraus ergibt sich die Abweisung der Beschwerde hinsichtlich der Erstbeschwerdegegnerin.

C. Datenverarbeitung hinsichtlich der Leistungsbeurteilung durch die Beschwerdeführerin

In weiterer Folge ergibt sich aus den vorhergehenden Erwägungen, dass die Beschwerdeführerin durch eine per Weisung »transparent« gestaltete Notengebung in der Form, dass sie die von ihr vorgenommene Leistungsbeurteilung über die Lernplattform laufend den betroffenen Schülerinnen und Schülern zugänglich machen muss, nicht in ihrem Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten verletzt wird. Die entsprechenden Daten, soweit sie überhaupt die Beschwerdeführerin betreffende Daten sind (was deshalb zu bejahen sein wird, weil Bewertungen, Gutachten udgl, stets auch Rückschlüsse auf die Person zulassen, die diese Angaben über einen Betroffenen, hier die Schülerin oder den Schüler, macht), dürfen gemäß § 8 Abs. 1 Z 4 und Abs. 3 Z 6 DSG 2000 im überwiegenden berechtigten Interesse des Zweitbeschwerdegegners verwendet werden, da sie sich ausschließlich auf die Ausübung der öffentlichen Funktion des Lehrerberufs durch die Beschwerdeführerin beziehen. Es beziehen sich auch weitere Daten betreffend die Ausübung des Lehrerberufes (wie: Name, akademische Grade und Titel, Tätigkeit an einer bestimmten Schule, unterrichtete Unterrichtsfächer und Klassen) auf eine solche öffentliche Funktion und dürfen daher die Beschwerdeführerin betreffend im gegebenen Zusammenhang durch die Schulbehörde verwendet werden.

D. Sonstige, die Beschwerdeführerin betreffende Datenverarbeitung

Soweit die Daten zu den Datenarten Name, öffentliche Funktion als Lehrerin an einer bestimmten Schule und dienstliche E-Mail-Adresse auf der Lernplattform verwendet werden, gilt das unter c. gesagte sinngemäß.

Daten betreffend die Systemverwendung (Protokoll- und Dokumentationsdaten wie Login-Zeiten, verwendete IP-Adressen, interne ID-Nummer) sind zwar die Beschwerdeführerin betreffende personenbezogene Daten, das Ermittlungsverfahren hat jedoch ergeben, dass diese nicht an andere Userinnen und User übermittelt sondern nur Mitarbeitern des Dienstleisters und von diesem bestellten Systemadministratoren zugänglich sind. Die Verwendung solcher Daten ist, soweit ihre Verwendung zweckgemäß auf die Kontrolle der Systemfunktionen und die Gewährleistung der technischen Datensicherheit beschränkt bleibt, gestützt auf § 14 Abs. 2, 4 und 5 DSG 2000 zulässig.

Für die Verwendung des Geburtsdatums der Beschwerdeführerin auf der Plattform kann allerdings in keinem der vorstehenden Rechtfertigungsgründe Deckung gefunden werden. Weder besteht ein direkter Konnex zwischen dem Geburtsdatum und der öffentlichen Funktion des Lehrerberufs, noch besteht eine ausdrückliche gesetzliche Grundlage für die Verwendung dieses Datums oder ein zwingender Zusammenhang mit deren Zwecken. Ob dieses Datum freiwillig von der Beschwerdeführerin selbst oder ohne ihr Zutun von einem bei der Erstbeschwerdegegnerin tätigen Systemadministrator eingegeben worden ist, kann dahingestellt bleiben. Es steht nämlich fest, dass die Beschwerdeführerin die Plattform nicht freiwillig, sondern nur unter Androhung und Anwendung disziplinarrechtlicher Sanktionen benützt hat. Daher kann auch eine durch sie selbst erfolgte Eingabe des Geburtsdatums nicht als »ohne Zwang abgegebene Willenserklärung« gemäß § 4 Z 14 DSG 2000 und damit als gültige Zustimmung zur Verwendung dieses Datums verstanden werden.

Hinsichtlich des Geburtsdatums war daher ein unzulässiger Eingriff in das Recht auf Geheimhaltung festzustellen.

v. Datenermittlung durch das Arbeitsmarktservice (K121.949/0023-DSK/2013, 6.9. 2013)

Sachverhalt:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass der Beschwerdegegner (das Arbeitsmarktservice, AMS; bzw. ein namentlich bezeichneter dortiger Mitarbeiter) einen »Arztbrief« des ihn behandelnden Arztes, dessen Vorlage ihm vom Beschwerdegegner aufgetragen worden sei, an eine Bezirkshauptmannschaft weitergegeben habe.

Der Beschwerdeführer ist von Beruf Kraftfahrer (Lkw) und im Besitz von Lenkberechtigungen der Klassen C und E. Er war im relevanten Zeitraum arbeitslos, beim Beschwerdegegner als arbeitsuchend gemeldet und bezog Leistungen der Arbeitslosenversicherung (Notstandshilfe). Weiters ist er Vater von minderjährigen Kindern, betreffend deren Unterhaltsansprüche eine Pflegschaftssache (außerstreitiges Unterhaltsverfahren) bei einem Bezirksgericht anhängig ist. In diesem Verfahren war über einen Antrag des Beschwerdeführers auf Herabsetzung der von ihm zu leistenden Unterhaltsbeiträge wegen verminderten Einkommens zu entscheiden.

Der Beschwerdeführer war wegen einer Anpassungsstörung mit längerer depressiver Reaktion bei einem Facharzt für Psychiatrie und Neurologie, in Behandlung. Er war laut diesem »nicht arbeitsfähig«. Der Beschwerdegegner verlangte vom Beschwerdeführer unter Hinweis auf mögliche Sanktionen (Sperre der Notstandshilfe) die Vorlage einer ärztlichen Bestätigung über seine Arbeitsfähigkeit, worauf der Beschwerdeführer einen vom Arzt erstellten schriftlichen Befund der Untersuchung vorlegte.

Später richtete das Bezirksgericht eine Anfrage an den Beschwerdegegner, die – neben Fragen nach dem Status des Beschwerdeführers bei der Arbeitssuche (ua nach der Zahl der Vermittlungsversuche) und der Höhe seiner Bezüge – folgendes Ersuchen enthält: »Sind Ermittlungsergebnisse zur Arbeitsfähigkeit (Gutachten) vorhanden, wird um Übersendung je einer Kopie gebeten.« Der Beschwerdegegner übermittelte daraufhin eine Kopie des Befunds des Facharztes an das Bezirksgericht.

Nachfolgend übersendete das Bezirksgericht den Akt an die Bezirkshauptmannschaft als für die Kinder des Beschwerdeführers zuständige Jugendwohlfahrtsbehörde zwecks Stellungnahme zu der Frage, ob aufgrund des Gesundheitszustandes des Beschwerdeführers die beantragte Einschränkung der Unterhaltsleistungen des Beschwerdeführers begründet sein könnte.

Daraufhin verständigte die Bezirkshauptmannschaft eine weitere Bezirkshauptmannschaft als die für den Beschwerdeführer nach seinem damaligen Wohnsitz zuständige Führerscheinbehörde, dass der Beschwerdeführer aufgrund der aus dem Befund hervorgehenden gesundheitlichen Beeinträchtigungen nicht arbeitsfähig sei. Diese Bezirkshauptmannschaft leitete ein Verfahren zur Entziehung, Einschränkung und Erlöschen der Lenkberechtigungen gemäß § 24 FSG ein und ordnete gemäß Abs. 4 leg cit zur Überprüfung der gesundheitlichen Eignung des Beschwerdeführers eine amtsärztliche Untersuchung an. Im weiteren Verlauf des führerscheinrechtlichen Verfahrens wurde nach Verlegung des Wohnsitzes des Beschwerdeführers die andere Bezirkshauptmannschaft örtlich zuständig und das Verfahren samt Verwaltungsakten an diese abgetreten.

Rechtliche Würdigung:
Der Beschwerdeführer hat ausdrücklich das Arbeitsmarktservice als Beschwerdegegner benannt.

A. Datenermittlung durch den Beschwerdegegner

§ 25 Abs. 1 Z 4 AMSG ermächtigt den Beschwerdegegner zur Verarbeitung von Gesundheitsdaten hinsichtlich gesundheitlicher Einschränkungen, die die Arbeitsfähigkeit oder die Verfügbarkeit infrage stellen oder die berufliche Verwendung berühren.

Aus § 8, § 10 Abs. 1 sowie § 16 Abs. 1 lit a) AlVG ergibt sich, dass für Zwecke der Beurteilung von Ansprüchen des Beschwerdeführers aus der Arbeitslosenversicherung bzw. für die Frage seiner Vermittlung auf dem Arbeitsmarkt die Ermittlung von Gesundheitsdaten denkmöglich von entscheidender Bedeutung war. Anders als im Fall des § 16 Abs. 1 lit. a) AlVG (Bezug von Krankengeld, Ruhen des Anspruchs auf Arbeitslosengeld und Notstandshilfe) ist bei der Frage der Arbeitsfähigkeit eines Arbeitslosen der Beschwerdegegner berechtigt, auch die Gründe der Arbeitsunfähigkeit, dh die Diagnose zu erfahren. Dies ergibt sich aus § 8 Abs. 2 AlVG, wonach auf Anordnung des Beschwerdegegners eine ärztliche Untersuchung, dh eine Befunderhebung durch einen vom AMS zu bestellenden und zu beauftragenden medizinischen Sachverständigen, vorzunehmen ist.

»Es ist nicht die Aufgabe des Sachverständigen, mit rechtlicher Wirkung über die den Gegenstand des Gutachtens bildende Fragestellung zu entscheiden. Der sachverständige Gutachter hat vielmehr dem zur Entscheidung befugten behördlichen Organ nur seine sachverständige Meinung zur Gutachtensfrage samt den Sachargumenten zu liefern, die das behördliche Organ in die Lage versetzen sollen, eine logisch nachvollziehbare Entscheidung zu treffen. Zu diesem Zweck müssen dem zur Entscheidung befugten Organ auch alle zur Begründung der sachverständigen Äußerung notwendigen Informationen zur Verfügung gestellt werden, d.h. im vorliegenden Fall auch das Ergebnis der Anamnese über den Gesundheitszustand des Betroffenen. Das Vorhandensein dieser Informationen bei der Behörde ist auch im Interesse der Nachprüfbarkeit der behördlichen Entscheidung – etwa im dienstrechtlichen Verfahren – unerlässlich.« (Bescheid der Datenschutzkommission vom 14. April 2010, K121.572/0003-DSK/2010).

Dies gilt sinngemäß auch für den Fall, dass die zuständige Behörde, hier der Beschwerdegegner, den Betroffenen, hier den Beschwerdeführer, im Sinne der Schnelligkeit und der Kostenersparnis ersucht oder auffordert, bereits vorhandene medizinische Befunde vorzulegen. Damit kann dahingestellt bleiben, inwieweit dies als Zustimmung zu werten wäre.

Der Beschwerdegegner war daher grundsätzlich gemäß § 9 Z 3 DSG 2000 gesetzlich ermächtigt, Gesundheitsdaten des Beschwerdeführers zu verarbeiten.

»Datenschutzrechtliche Beschwerden sind nicht geeignet, in der Sache vor andere Behörden gehörende Rechtsfragen [...] prüfen zu lassen. Grundsätzlich besteht ein – im Fall von Verwaltungsübertretungen insbesondere durch § 25 Abs. 1 iVm § 26 Abs. 1 VStG, im allgemeinen Verwaltungsverfahren durch die §§ 37 und 39 Abs. 2 AVG sowie besondere Zuständigkeitsbestimmungen zum Ausdruck kommendes – berechtigtes Interesse der zuständigen Behörde an der Verwendung personenbezogener Daten, [...] welches das Interesse der Betroffenen an der Geheimhaltung ihrer personenbezogenen Daten überwiegt, sodass gemäß § 8 Abs. 1 Z 4 bzw. § 8 Abs. 4 Z 3 DSG 2000 eine Verletzung von nach § 1 Abs. 1 leg. cit. bestehenden schutzwürdigen Geheimhaltungsinteressen nicht vorliegt. Als Maßstab für eine Beurteilung der Zulässigkeit der Datenermittlung in solchen Verfahren verbleibt für die Datenschutzkommission das Übermaßverbot als Ausdruck des in § 1 Abs. 2 und § 7 Abs. 3 DSG 2000 normierten

Verhältnismäßigkeitsgrundsatzes: Wenn es denkmöglich ist, dass die von einer in der Sache zuständigen Behörde ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet sind, ist die Zulässigkeit der Ermittlung aus datenschutzrechtlicher Sicht gegeben.« (Bescheid der Datenschutzkommission vom 29. November 2005, K121.046/0016-DSK/2005).

Für die Frage, ob der Beschwerdeführer gesundheitlich (durch eine Anpassungsstörung mit längerer depressiver Reaktion) arbeitsfähig und für bestimmte Stellen vermittelbar war, ist die Ermittlung von Gesundheitsdaten denkmöglich entscheidend. Eine alternative, weniger eingriffsintensive Methode, ein gelinderes Mittel im Sinne des § 7 Abs. 3 DSG 2000, zur sicheren Erreichung des Verfahrenszieles (Gewinnung von Erkenntnissen in der Frage der Arbeitsfähigkeit des Beschwerdeführers) ist nicht erkennbar und vom Beschwerdeführer im Verfahren auch nicht aufgezeigt worden. Eine (neuerliche) ärztliche Untersuchung gemäß § 8 Abs. 2 AlVG wäre nicht nur gleich eingriffsintensiv im datenschutzrechtlichen Sinne sondern auch mit höheren Kosten verbunden gewesen.

Der Beschwerdegegner hat den Beschwerdeführer durch die Ermittlung der Daten im Befund daher nicht in seinem Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten verletzt.

B. Übermittlung des Befunds an das Bezirksgericht

Dieser Übermittlung lag ein schriftliches Ersuchen (»Anfrage«) des Bezirksgerichts zugrunde. Eine derartige Anfrage eines anderen, hoheitlich tätigen Staatsorgans löst gemäß Art. 22 B-VG eine Pflicht zur Leistung von Amtshilfe aus. Gemäß § 9 Z 4 DSG 2000 kann die Amtshilfepflicht auch die Übermittlung (»Verwendung«) von sensiblen Daten rechtfertigen.

Da im Beschwerdefall direkt und konkret nach Kopien vorhandener (schriftlicher) Ermittlungsergebnisse wie Gutachten gefragt wurde, ist ebenfalls kein gelinderes Mittel im Sinne des § 7 Abs. 3 DSG 2000 zur pflichtgemäßen Erfüllung des Ersuchens erkennbar. Für den Beschwerdegegner war auch erkennbar, dass die Frage einer Arbeitsfähigkeit des Beschwerdeführers für das Bezirksgericht in einer Unterhaltssache denkmöglich von Bedeutung war. Die Bedingungen des § 7 Abs. 2 Z 2 DSG 2000 waren somit erfüllt.

Der Beschwerdegegner hat den Beschwerdeführer durch die Übermittlung der Daten im Befund an das Bezirksgericht daher ebenfalls nicht in seinem Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten verletzt.

C. weitere Übermittlungsvorgänge

Es konnte nicht festgestellt werden, dass der Befund vom Beschwerdegegner an andere Staatsorgane als das Bezirksgericht übermittelt worden ist. Für den Daten- bzw. Informationsaustausch zwischen dem Bezirksgericht (das gemäß § 31 Abs. 2 DSG 2000 überhaupt außerhalb der Zuständigkeit der Datenschutzkommission liegt) und den Bezirkshauptmannschaften kann der Beschwerdegegner als datenschutzrechtlicher Auftraggeber jedoch nicht belangt werden.

Die Beschwerde war daher gemäß § 31 Abs. 7 DSG 2000 insgesamt als unbegründet abzuweisen.

8.1.3 Recht auf Löschung und Richtigstellung

a. Verpflichtung zur Löschung von Investorenwarnungen (K121.746/0002-DSK/2012, 18. 1. 2012)

Sachverhalt:

Die Beschwerdeführerin behauptet eine Verletzung im Recht auf Löschung personenbezogener Daten dadurch, dass die Beschwerdegegnerin (die Finanzmarktaufsichtsbehörde) sich geweigert habe, eine die Beschwerdeführerin betreffende und auf der Website www.fma.gv.at öffentlich abrufbare Investorenwarnung (gem § 92 Abs. 11 WAG 2007) zu löschen. Hinsichtlich der Rechtmäßigkeit der Investorenwarnung sei ein Überprüfungsverfahren beantragt und von der Beschwerdegegnerin mit Bescheid abschlägig entschieden worden. Diesbezüglich seien Beschwerden beim VfGH und VwGH anhängig. Die Daten auf besagter Website seien objektiv unrichtig, da die Beschwerdeführerin in Österreich keine Wertpapierdienstleistungen anbiete und auch gewisse gesellschaftsrechtliche Verbindungen falsch dargestellt würden. Das Löschungsbegehren (in eventu Richtigstellungsbegehren) aus April 2011 sei im Juni 2011 mit der Begründung abgelehnt worden, wie bereits im ergangenen Bescheid dargelegt bestehe keine Rechtsgrundlage für die Entfernung der Warnmeldung, darüber hinaus habe man sich auf den Dokumentationszweck gem § 22 Abs. 4 FMABG berufen.

Rechtliche Würdigung:

Die DSK ging zunächst der Frage nach, welche gesetzliche Zuständigkeit und Befugnis die angerufene Behörde hat, über die Rechtmäßigkeit einer Warnmeldung, also eine öffentliche Bekanntgabe von Daten über die Beschwerdeführerin, zu entscheiden. Die Antwort dafür wurde aus dem Erkenntnis des VfGH vom 12. März 2009, G 164/08, gewonnen. Damit wurde der erste Satz des § 4 Abs. 7 des Bankwesengesetzes (BWG), BGBl 1993/532 in der Fassung BGBl I 2001/97, als verfassungswidrig aufgehoben.

Die Bestimmung des § 4 Abs. 7 BWG lautete dabei wie folgt: »(7) Die FMA ist berechtigt, im Einzelfall durch Kundmachung im ‚Amtsblatt zur Wiener Zeitung' oder in einem anderen bundesweit verbreiteten Bekanntmachungsblatt die Öffentlichkeit zu informieren, dass ein namentlich genanntes Unternehmen zur Vornahme bestimmter Bankgeschäfte nicht berechtigt ist. Die FMA hat auf individuelle Anfrage in angemessener Frist Auskünfte über den Konzessionsumfang von Kreditinstituten zu erteilen. Die FMA hat bis zum 1. Jänner 2004 eine Datenbank aufzubauen, die Informationen über den aktuellen Umfang der bestehenden Konzessionen der Kreditinstitute enthält, und hat über Internet eine Abfrage dieser Daten zu ermöglichen.«

In seiner Entscheidung hat der VfGH darauf hingewiesen, dass er wiederholt ausgesprochen habe, dass Finanzinstitute ihre Tätigkeit in einem volkswirtschaftlichen Schlüsselbereich ausüben, von dessen Funktionieren weite Teile der Volkwirtschaft abhängig sind, und dass eine besondere Schutzbedürftigkeit der Sparer und sonstigen Gläubiger von Kreditunternehmungen besteht. Demnach bestünden keine grundsätzlichen Bedenken gegen eine Norm wie die des § 4 Abs. 7 BWG, die offensichtlich den Zweck verfolgt, durch eine rasche Information der Öffentlichkeit über rechtswidrige Geschäftspraktiken Schäden vor allem bei Anlegern zu verhindern und das Vertrauen in die Funktionsfähigkeit des gesamten Finanzsektors zu stärken. Es sei auch nicht zu bezweifeln, dass es die besondere Situation am Kapitalmarkt es in bestimmten Situationen erforderlich mache oder zumindest zweckmäßig erscheinen lässt, zum Schutz von Anlegern sofort und ohne vorherige Einbindung des betroffenen Unternehmens Meldungen dieser Art zu veröffentlichen. Der Gerichtshof hegte aber Zweifel an der verfassungsrechtlichen Zulässigkeit einer Regelung der vorliegenden Art, wenn sie eine Kundmachung dieses Inhaltes zulässt, ohne dass für das betroffene Unternehmen die Möglichkeit besteht, die eigene Position darzulegen und den Wahrheitsgehalt dieser Kundmachung überprüfen zu lassen. Die damalige Rechtslage scheine nämlich darauf hinauszulaufen, dass der Veröffentlichung kein rechtsförm-

licher, mit Rechtsmitteln bekämpfbarer Akt (Bescheid oder Verordnung) zugrunde liege oder nachzufolgen habe und dass die Berechtigung der Veröffentlichung bzw. der Aufrechterhaltung der ‚Warnmeldung' auch nicht in einem nachfolgenden Verfahren (mit Parteiengehör) überprüfbar ist. Auch scheine nicht vorgesehen zu sein, dass ein Widerruf der ‚Warnmeldung' vorzunehmen ist. Der Rechtsschutz dürfte sich auf die Amtshaftung beschränken.

Die Bedenken des Gerichtshofes betrafen also sowohl das Sachlichkeitsgebot des Gleichheitssatzes als auch das Rechtsstaatsprinzip, wenn eine Information nach Art des § 4 Abs. 7 erster Satz BWG veröffentlicht werden darf, ohne dass von der Rechtsordnung ein adäquates Instrumentarium der Überprüfung und – für den Fall der unzutreffenden Information – der Folgenbeseitigung zur Verfügung gestellt wird.

Sowohl die Tatsachenannahmen der Behörde als auch ihre rechtliche Beurteilung sind aber mit einem Fehlerrisiko behaftet. Der Gerichtshof hatte schon im Prüfungsbeschluss darauf hingewiesen, dass es durchaus strittig sein kann, ob die von einem Unternehmen beabsichtigte oder schon aufgenommene Geschäftstätigkeit einer Konzession nach dem BWG bedarf bzw. ob eine vorhandene Konzession (auch) diese Geschäftstätigkeit abdeckt. Strittig kann aber auch sein, ob das betroffene Unternehmen überhaupt eine einschlägige Tätigkeit beabsichtigt oder entfaltet. Der Gerichtshof bleibt dabei, dass unter solchen Umständen sowohl das Sachlichkeitsgebot des Gleichheitssatzes als auch das Rechtsstaatsprinzip verletzt sind, wenn eine solche, ein einzelnes Unternehmen betreffende Information veröffentlicht werden darf, ohne dass diesem Unternehmen von der Rechtsordnung ein adäquates Instrumentarium zur Verfügung gestellt würde, die Information auf ihre Berechtigung überprüfen, evtl öffentlich korrigieren sowie allfällige Folgen einer rechtswidrigen Information beseitigen zu lassen.

Dass mit den Mitteln des Datenschutzrechtes der adäquate Rechtsschutz gegen behaupteter maßen falsche oder unangebrachte Informationen nach § 4 Abs. 7 BWG gewährleistet wäre, konnte der Gerichtshof nicht finden: Die mit Beschwerde nach § 31 Abs. 2 DSG 2000 erreichbare »Richtigstellung« und »Löschung« bezog sich nur auf Dateien und schied als tauglicher Rechtsbehelf gegen Warnmeldungen in einer Zeitung daher schon deswegen aus, weil – wie es auch der Anlassfall dieses Verfahrens gezeigt habe – die Veröffentlichung von Informationen nach § 4 Abs. 7 Satz 1 BWG auch ohne Rückgriff auf Dateien iSd DSG 2000 erfolgen kann, eine Konstellation, die sogar den Regelfall darstellen dürfte, da es typischerweise um Unternehmen geht, die nicht in der Liste der konzessionierten Unternehmen zu finden sind. Aber auch der in § 31 Abs. 2 DSG 2000 normierte Schutz gegen Verletzungen des Rechts auf Geheimhaltung kommt als adäquater Rechtsbehelf gegen Meldungen nach § 4 Abs. 7 BWG nicht in Betracht, weil zum einen die Frage, ob ein Unternehmen die – nach Auffassung der FMA – erforderliche Konzession besitzt, keine Tatsache ist, die der Geheimhaltung unterliegt, und zum anderen mit diesem Rechtsbehelf kein Widerruf und keine Richtigstellung einer falschen oder unangebrachten Warnmeldung erreicht werden kann.

In Reaktion auf diese Entscheidung des VfGH hat nun der Gesetzgeber mit § 92 Abs. 11 WAG 2007 die Kundmachung von Warnmeldungen insofern auf eine neue Basis gestellt, als er ausdrücklich das Mittel der automationsunterstützten Datenverwendung (»Kundmachung im Internet«) in Verbindung mit einem auf Löschung dieser Daten (umschrieben als »aus dem Internetauftritt zu entfernen«) gerichteten Rechtsschutzverfahren vorsieht.

Daraus ergibt sich im Ergebnis, dass die FMA alleine zur Entscheidung mittels Feststellungsbescheids darüber berufen ist, ob die Voraussetzungen für eine Veröffentlichung im Internet gegeben sind. Durch diese Feststellung wird über das Vorliegen der Veröffentlichungsvoraussetzungen – als Hauptfrage – von der hiefür nach der Bestimmung des § 92 Abs. 11 WAG

zuständigen Behörde abgesprochen. Ob diese Veröffentlichungsvoraussetzungen vorliegen, kann von der Datenschutzkommission nur im Rahmen einer Vorfragenbeurteilung gem § 38 AVG geprüft werden. Jede andere Auslegung des Gesetzes würde zu einer konkurrierenden Zuständigkeit (zwei Behörden zuständig zur Entscheidung über dieselbe Hauptfrage) führen und § 92 Abs. 11 WAG 2007 damit im Lichte von Art 83 Abs. 2 B-VG (Recht auf Entscheidung durch den »gesetzlichen Richter«) und § 1 Abs. 5 DSG 2000 (verfassungsrechtlich verankerte Zuständigkeit der Datenschutzkommission zur Entscheidung über Löschungsansprüche gegenüber Verwaltungsbehörden) einen verfassungswidrigen Inhalt unterstellen. Der Bescheid der Beschwerdegegnerin aus April 2011, mit dem die Rechtmäßigkeit der Warnmeldung rechtskräftig festgestellt worden ist, bindet daher als Vorfragenentscheidung gem § 38 AVG die Datenschutzkommission. Dazu ist auch die Rsp der Datenschutzkommission vom Übermaßverbot zu berücksichtigen (z. B. Bescheid vom 28. 2. 2003, K120.806/002-DSK/2003, stRspr). Das hier zur Frage der Ermittlung (und damit der Geheimhaltung von Daten) Gesagte gilt mutatis mutandis auch in der Frage der Löschung des Dateninhalts einer Kundmachung, wenn diese Kundmachung, so wie hier, in den gesetzlichen Zuständigkeitsbereich einer anderen Behörde fällt. Eine Überprüfung, die eine inhaltliche Korrektur des oben zitierten Bescheids bedeuten würde, ist der Datenschutzkommission damit jedenfalls aus Zuständigkeitsgründen verwehrt.

Wenngleich die Prüfung der Rechtmäßigkeit der verfahrensgegenständlichen Kundmachung nicht erfolgen darf, war doch zu fragen, ob sich ein Löschungsanspruch nicht aus der Dauer der Veröffentlichung im Internet ergibt. Dies deshalb, als Daten, sobald sie für den Zweck der Datenanwendung nicht mehr benötigt werden sollten, gem § 27 Abs. 1 DSG 2000 als unzulässig verarbeitete Daten gelten und – von einer im vorliegenden Fall nicht relevanten Ausnahme abgesehen – zu löschen sind. Ausgehend von der auch vom VfGH in dem obzitierten Erkenntnis erwähnten Tatsache, dass Finanzinstitute ihre Tätigkeit in einem volkswirtschaftlichen Schlüsselbereich ausüben, von dessen Funktionieren weite Teile der Volkwirtschaft abhängig sind, und dass eine besondere Schutzbedürftigkeit der Sparer und sonstigen Gläubiger von Kreditunternehmungen besteht und dass es insb die besondere Situation am Kapitalmarkt in bestimmten Situationen erforderlich mache oder zumindest zweckmäßig erscheinen lasse, zum Schutz von Anlegern sofort und ohne vorherige Einbindung des betroffenen Unternehmens Meldungen dieser Art zu veröffentlichen, kann gesagt werden, dass ein im Internet erfolgter berechtigter Warnhinweis aufgrund seiner Warnfunktion vor (ehemals oder noch immer) unseriösen Anbietern im Bereich der Wertpapieranlagengeschäfte auch bei Wegfall der ursprünglichen Kundmachungsvoraussetzungen aus datenschutzrechtlicher Sicht nicht sofort gelöscht werden muss. Zum einen nimmt die gegenständliche Kundmachung im Internet ausdrücklich auf das Datum Bezug, sodass sich jeder Interessent über die Aktualität der Kundmachungsvoraussetzungen informieren kann, zum anderen besteht der Zweck des Warnhinweises aus Sicht der Datenschutzkommission auch darin, eine gewisse Zeit hindurch Interessenten aus Gründen des Verbraucherschutzes über ein solches Verhalten in der Vergangenheit zu informieren. Ein Kundmachungszeitraum von knapp einem Jahr ist war aus Sicht der Datenschutzkommission jedenfalls nicht als unverhältnismäßig anzusehen.

Die Beschwerde war daher als unbegründet abzuweisen.

b. Löschung einer KPA-Eintragung (K121.885/0011-DSK/2012, 14. 12. 2012)

Sachverhalt:

Die Beschwerdeführerin behauptet eine Verletzung im Recht auf Löschung dadurch, dass die Beschwerdegegnerin (eine Bezirkshauptmannschaft) ihr Löschungsbegehren vom Juni 2012 betreffend die Löschung einer KPA-Eintragung mit nachfolgenden Schreiben zu Unrecht abgelehnt habe. Sie stellte den Antrag, diese Rechtsverletzung festzustellen.

Gegen die Beschwerdeführerin wurden im Jahr 2007 Vorerhebungen im Dienste der Strafjustiz wegen des Verdachts der Verleumdung geführt. Nach einer Strafanzeige folgte nach Antrag der Staatsanwaltschaft ein gerichtliches Hauptverfahren vor dem zuständigen Landesgericht, das die Beschwerdeführerin mit Urteil aus Jänner 2009 der Verleumdung gem § 297 Abs. 1 2. Fall StGB für schuldig befunden hat.

Dazu wird seit Mai 2008 bis heute ein Eintrag unter den Personendaten der Beschwerdeführerin in der Datenanwendung gem § 57 Abs. 1 Z 1 SPG (Zentrale Informationssammlung der Sicherheitsbehörden – kriminalpolizeilicher Aktenindex) verarbeitet.

Das Löschungsbegehren der Beschwerdeführerin aus Juni 2012 lehnte die Beschwerdegegnerin mit der Begründung ab, die Verarbeitung dieser Daten sei weder unzulässig noch rechtswidrig, da die Beschwerdeführerin rechtskräftig verurteilt worden sei. Der Verdacht, der Anlass zur Eintragung gegeben habe, sei also bestätigt worden.

Rechtliche Würdigung:
Wie sich aus den Sachverhaltsfeststellungen ergibt, ist die bestehende KPA-Eintragung nicht unrichtig. Der Verdacht einer strafbaren Handlung wurde sogar durch das im Anschluss an die eingeleiteten Ermittlungen im Dienste der Strafrechtspflege durchgeführte gerichtliche Hauptverfahren bestätigt.

Das Recht auf Löschung wird im Fall der sicherheitspolizeilichen Datenanwendung KPA einfachgesetzlich durch die §§ 57 bis 63 SPG geregelt.

Die Ansicht der Beschwerdeführerin, durch die Bestätigung des Anfangsverdachts in Form der Verurteilung (und damit der Aufnahme eines entsprechenden Eintrags ins Strafregister) werde die KPA-Vormerkung gleichsam »überflüssig«, findet im Gesetz keine Deckung. Der KPA dokumentiert die sicherheits- bzw. kriminalpolizeiliche Seite eines Ermittlungsverfahrens, insb durch Angabe der ermittelnden Dienststelle oder Einheit der Bundespolizei und der verantwortlichen Sicherheitsbehörde, der rechtlichen Qualifikation des Anfangsverdachts sowie der Bezug habenden Aktenzahl. Das Strafregister dokumentiert dagegen die gerichtliche Verurteilung, insb das Gericht, dessen AZ sowie die verhängte Strafe. Wird der entsprechende Anfangsverdacht nicht widerlegt sondern bestätigt, so gilt für die KPA-Daten grundsätzlich die auf Zeitablauf abstellende Löschungsvorschrift des § 58 Abs. 1 Z 6 SPG.

Die fünfjährige Löschungsfrist für eine im Mai 2008 erfolgte KPA-Eintragung war im Juni 2012 (Zeitpunkt der Ablehnung des Löschungsbegehrens) noch nicht abgelaufen. Weitere besondere Gründe, die etwa eine vorzeitige Löschung der Daten (wegen Wegfalls der Notwendigkeit ihrer Verarbeitung gem § 63 Abs. 1 SPG) darlegen könnten, hat die Beschwerdeführerin nicht aufgezeigt und haben sich auch im Zuge des Ermittlungsverfahrens nicht ergeben.

Die Beschwerdegegnerin hat die Löschung der KPA-Vormerkung der Beschwerdeführerin im Juni 2012 daher zur Recht abgelehnt, die dagegen erhobene Beschwerde war als unbegründet abzuweisen.

c. Löschung von Daten aus einem Finanzakt (K121.979/0014-DSK/2013, 6. 9. 2013)

Sachverhalt:
Die Beschwerdeführerin führte aus, dass der Beschwerdegegner (ein Finanzamt) ihrem Löschungsersuchen gemäß § 27 DSG 2000 aus April 2013 nicht entsprochen habe. Sie erhebe nunmehr Beschwerde wegen Verletzung des Rechts auf Löschung, wobei die strittigen Daten, insb Daten zu ihrem Sexualleben, sowohl als Papierakt als auch als elektronischer Akt vorlägen.

Der Beschwerdegegner nahm eine vom Landeskriminalamt (LKA) übermittelte Anzeige wegen des Verdachts der illegalen Prostitution zum Anlass, diese Information in abgabenrechtliche Verfahren betreffend die Beschwerdeführerin für bestimmte Jahre miteinzubeziehen. Die auf Basis dieser Informationen ergangenen Einkommensteuerbescheide des Beschwerdegegners wurden im Instanzenzug vom Unabhängigen Finanzsenat behoben. Die dagegen vom Beschwerdegegner erhobene Amtsbeschwerde wurde mit Erkenntnis des VwGH als unbegründet abgewiesen.

Sämtliche Daten das Sexualleben der Beschwerdeführerin betreffend, welche der Beschwerdegegner den erwähnten Einkommensteuerbescheiden zugrunde legte, sind nur im Betriebsprüfungs-Arbeitsbogen aufbewahrt, welcher als herkömmlicher behördlicher Papierakt angelegt wurde. Es erfolgte keine elektronische Speicherung von Daten betreffend das Sexualleben der Beschwerdeführerin. Auch die zitierte Amtsbeschwerde wurde nicht elektronisch gespeichert. In den elektronisch gespeicherten Dokumenten wird lediglich auf Dokumente des Papierakts verwiesen, was der behördeninternen Wiederauffindbarkeit des Papieraktes dienen soll.

Rechtliche Würdigung:
A. Zum Umfang der Prüfkompetenz der Datenschutzkommission:

§ 1 Abs. 3 in Verbindung mit § 31 Abs. 1 und 2 DSG 2000 legt die Prüfkompetenz der Datenschutzkommission in Beschwerdeverfahren fest. Demnach hat sie nicht zu prüfen, ob irgendein (verfassungsrechtlich gewährleistetes) Recht verletzt wurde sondern nur, ob ein Beschwerdeführer in seinem (verfassungsrechtlich gewährleisteten) Recht auf Auskunft oder – soweit die Voraussetzungen des § 31 Abs. 2 DSG 2000 vorliegen – in seinem (verfassungsrechtlich gewährleisteten) Recht auf Richtigstellung oder Löschung verletzt wurde.

Soweit die Beschwerdeführerin vorbringt, dass ihr ein auf Art. 8 EMRK gestütztes (verfassungsrechtlich gewährleistetes) Recht auf Löschung zukommt, ist dieses Vorbringen somit nur insoweit zu prüfen, als es auch in § 1 Abs. 3 Z 2 DSG 2000 Deckung findet (vgl dazu auch die Rechtsprechung des VfGH, wonach aus Art. 8 EMRK hinsichtlich der Löschungsverpflichtung kein weiter reichendes Recht abzuleiten ist als aus der Verfassungsbestimmung des § 1 Abs. 3 DSG 2000; VfSlg 18.092/2007).

B. Zur Löschung der automationsunterstützt verarbeiteten Daten:

Es werden keine das Sexualleben der Beschwerdeführerin betreffenden Daten automationsunterstützt gespeichert, sodass sich die Beschwerde in diesem Punkt daher als unbegründet erweist.

Wenn sie darüber hinaus geltend macht, dass die (sonstigen) elektronisch gespeicherten Daten aufgrund des Erkenntnisses des VwGH nicht mehr benötigt würden, ist auf die Rechtsprechung der Datenschutzkommission zu verweisen, wonach – unter Bezugnahme auf § 6 Abs. 1 Z 5 DSG 2000 – Daten auch nach Abschluss eines Verfahrens aufbewahrt werden können, um eine Nachvollziehbarkeit behördlichen Handelns zu gewährleisten (vgl dazu etwa den Bescheid vom 20. Jänner 2010, GZ K121.553/0003-DSK/2010). Folglich kann unter Berücksichtigung der Tatsache, dass – wie der Beschwerdegegner richtig ausführt – die Wiederaufnahme des verwaltungsgerichtlichen Verfahrens nicht auszuschließen ist und die in § 45 Abs. 2 VwGG normierte Frist noch nicht abgelaufen ist, der Argumentation des Beschwerdegegners, die weitere Aufbewahrung der Daten sei aus Gründen der Dokumentation behördlichen Handelns weiterhin erforderlich, nicht entgegengetreten werden.

C. Zur Löschung der im Papierakt aufbewahrten Daten:

C.1 zur Möglichkeit des Beschwerdegegners die vom LKA übermittelten Daten zu verwenden

Die Beschwerdeführerin führt aus, dass mittlerweile festgestellt worden sei, dass das LKA die Daten betreffend ihr Sexualleben rechtswidrig erlangt habe bzw. dass diese in einer Art. 3 EMRK widersprechenden Weise ermittelt wurden und der Beschwerdegegner diese Daten folglich dem abgabenrechtlichen Verfahren nicht hätte zugrunde legen dürfen.

Diesem Vorbringen ist zu erwidern, dass nach der ständigen Rechtsprechung des VwGH im Abgabenverfahren auch Beweismittel verwendet werden dürfen, die andere Behörden erhoben haben; eine unmittelbare Beweisaufnahme ist im Abgabenverfahren nicht erforderlich (vgl dazu das Erkenntnis vom 31. März 2011, Zl. 2009/15/0199). Dem Verfahren zur Abgabenerhebung nach den Bestimmungen der BAO ist ein Beweisverwertungsverbot grundsätzlich fremd. Nach § 166 BAO kommt nämlich als Beweismittel im Abgabenverfahren alles in Betracht, was zur Feststellung des maßgebenden Sachverhaltes geeignet und nach Lage des einzelnen Falles zweckdienlich ist. In stRsp hat der VwGH daher ausgesprochen, dass die Verwertbarkeit eines Beweismittels auch dadurch nicht ausgeschlossen wird, dass es durch eine Rechtsverletzung in den Besitz der Abgabenbehörde gelangte (vgl dazu etwa das Erkenntnis vom 17. November 2010, Zl. 2007/13/0078, mwN).

Der Beschwerdegegner durfte sohin die vom LKA übermittelten Daten dem abgabenrechtlichen Verfahren zugrunde legen.

C.2 in der Sache

§ 4 Z 6 DSG 2000 definiert »Datei« als strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind. Laut VwGH (Erkenntnis vom 21. Oktober 2004, Zl. 2004/06/0086) wie VfGH (Erkenntnis vom 15. Dezember 2005, Zl. B 1590/03) genügt ein Akt oder Aktenkonvolut bzw. ein nicht personenbezogen strukturierter Papierakt den gesetzlichen Anforderungen an eine Datei gemäß § 4 Z 6 DSG 2000 nicht. Es kann daher auf Grundlage datenschutzrechtlicher Bestimmungen, insb des § 27 DSG 2000, keine »Löschung« des Aktes oder darin enthaltener Angaben zu Personen verlangt werden.

Da das Vorbringen des Beschwerdegegners zu dem Schluss führt, dass der die Beschwerdeführerin betreffende vorhandene Betriebsprüfungs-Arbeitsbogen keine vorgegebene inhaltliche Struktur aufweist (vgl dazu die Ausführungen des VwGH in dem bereits zitierten Erkenntnis vom 21. Oktober 2004: »Behördliche oder gerichtliche ‚Akten' werden in Österreich typischerweise derart gebildet, dass die verschiedenen Geschäftsstücke, welche die Sache betreffen, entweder in einen Umschlag (Mappe, Ordner oder dergleichen) in der Regel in chronologischer Reihenfolge aufgenommen werden, oder aber auch (so etwa beispielsweise im Bereich der Bundesministerien) Geschäftsstücke nach dem Fortgang des Verfahrens jeweils in eigene Referatsbögen (mit eigenen Zahlen) eingelegt werden und daraus dann die die Sache betreffenden Aktenkonvolute gebildet werden«) und daher keine »Datei« ist, kommt der Beschwerde in Bezug auf den Papierakt ebenfalls keine Berechtigung zu. Entgegen der Ansicht der Beschwerdeführerin wird ein Papierakt auch durch die Anführung der DVR-Nummer des Auftraggebers auf inliegenden Schriftstücken bzw. durch den Verweis in elektronisch gespeicherten Dokumenten auf den Papierakt noch nicht zur Datei, weil dieser – trotz dieser Verweise – keine inhaltliche Struktur aufweist, die es ermöglicht, Daten nach zumindest einem Suchkriterium zu finden.

Die Beschwerde war folglich abzuweisen.

8.2 Kontrollverfahren nach § 30 DSG 2000

Zusätzlich zur unter I. dargestellten förmlichen Rechtsdurchsetzung kann sich nach § 30 Abs. 1 DSG 2000 jedermann wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten nach dem DSG 2000 mit einer Eingabe an die DSK wenden. Dies führt in der Regel zur Durchführung eines so genannten Kontrollverfahrens (auch als »Ombudsmannverfahren« bezeichnet).

Bei vorabkontrollpflichtigen Datenanwendungen kann ein solches auch ohne Vorliegen einer Eingabe oder auch nur eines konkreten Verdachts durchgeführt werden. Die Durchführung eines solchen Verfahrens ist (anders als beim Beschwerdeverfahren) unabhängig vom geltend gemachten Recht (Pflicht) bzw.. dem angesprochenen Auftraggeber zulässig, und zwar auch dann, wenn die DSK alternativ auch zur förmlichen Rechtsdurchsetzung zuständig wäre.

Ziel ist nach § 30 Abs. 6 DSG 2000 die Herbeiführung eines rechtmäßigen Zustands. Dazu können nötigenfalls auch – nicht unmittelbar verbindliche – Empfehlungen ausgesprochen werden. Häufig kann aber auch ohne den Einsatz dieses Mittels im Zuge solcher Verfahren eine datenschutzrechtlich befriedigende Situation hergestellt werden, wenn sich die Eingabe nicht schon von vornherein als unbegründet erweist.

Im Berichtszeitraum scheinen aus diesem Bereich die folgenden Fälle bzw.. Fallgruppen besonders erwähnenswert:

a. Empfehlung zu in AGB enthaltenen Zustimmungserklärungen (K212.766/0010-DSK/2012, 13. 7. 2012)

Sachverhalt:

Der Einschreiter führte aus, ein österreichisches Unternehmen hole in seinen allgemeinen Geschäftsbedingungen für ein Produkt (AGB), veröffentlicht auf dessen Website, Zustimmungen von den Kunden für die Verwendung ihrer Daten u. a.. für Gewinnspiele und Spendenaktionen ein. Der Einschreiter sieht sich im Ergebnis dadurch in seinem Recht auf Geheimhaltung verletzt, dass er durch die Einbindung dieser Zustimmungserklärung in die AGB den dort genannten Datenverwendungen zustimmen muss.

Eine von den AGB getrennte Annahme dieser Zustimmungserklärung im Internet ist nicht möglich, da zum Abschluss der Bestellung folgender Text durch Tickbox angenommen werden muss: »Ich bestätige hiermit, den Inhalt der AGB ... und insbesondere die in deren Punkt 6 enthaltene Zustimmung zur Verarbeitung und Übermittlung meiner Daten zur Kenntnis genommen zu haben, und erkläre mich damit einverstanden.« Der Abschluss des Vertrages ohne Abgabe der Zustimmungserklärung ist daher nicht möglich.

Rechtliche Würdigung:

Der Auftraggeber stützt die Zulässigkeit der in Klausel 6 der AGB genannten Datenverwendungen auf eine ausdrückliche datenschutzrechtliche Zustimmung (iSd § 4 Z 14 DSG 2000) gem § 7 Abs. 1 iVm § 8 Abs. 1 Z 2 DSG 2000. Eine gültige datenschutzrechtlichen Zustimmung iSd § 4 Z 14 DSG 2000 liegt nur vor, wenn die Willenserklärung u. a.. ohne Zwang abgegeben wurde. Die Freiwilligkeit bei der Abgabe der Zustimmungserklärung ist eine Grundvoraussetzung für den rechtsgültigen Eingriff in das Grundrecht auf Datenschutz (§ 1 DSG 2000).

Betreffend Zustimmungserklärungen in AGBs führte das Rundschreiben des BKA-VD aus August 1985 (zur gleich gelagerten alten Rechtslage) aus:

»1. Eine ausdrückliche Zustimmung des Betroffenen kann keinesfalls dann vorliegen, wenn sie bloß als Bestandteil von AGB vom Betroffenen zur Kenntnis genommen wurde. Vielmehr liegt eine ‚ausdrückliche' schriftliche Zustimmung nur dann vor, wenn der Betroffene sein Einverständnis zur Datenübermittlung getrennt von etwaigen sonstigen vertraglichen Vereinbarungen gegeben hat.

2.a) Hinsichtlich der Form der Zustimmungserklärung ist daher zu verlangen, dass diese deutlich vom übrigen Text eines Formulars, eines Schriftstückes u. dgl. abgesetzt ist. Hinweise auf allgemeine Geschäftsbedingungen, auf Angaben in anderen Dokumenten, die nicht Bestandteil des unterzeichneten Papiers sind, sind nicht zulässig.

...

c) Die Zustimmungserklärung bedarf jedenfalls einer gesonderten Unterzeichnung: die einheitliche Unterzeichnung eines Formulars, in dem neben anderen Erklärungen auch die Zustimmungserklärung enthalten ist, reicht nicht aus. Es ist daher in solchen Fällen jedenfalls erforderlich, die Zustimmungserklärung vom übrigen Formulartext derart zu trennen, dass eine gesonderte Unterfertigung der Zustimmungserklärung und der sonstigen vom Formular vorgesehenen Angaben möglich ist.«

Auch die »Stellungnahme 15/2011 zur Definition von Einwilligung« (iSd Datenschutz-Richtlinie 95/46/EG) der Art. 29 Datenschutzgruppe, WP 187, aus Juli 2011, führt aus, dass die Einwilligung ohne Zwang und für den konkreten Fall erfolgen muss, weshalb eine pauschale Einwilligung ohne genaue Festlegung des Zwecks nicht rechtmäßig ist. Diese Informationen sollten nicht in den allgemeinen Geschäftsbedingungen des Vertrags stehen, sondern es sollten stattdessen spezielle Einwilligungsklauseln gesondert von den allgemeinen Geschäftsbedingungen verwendet werden.

Auch im konkreten Fall war es für den Kunden nicht möglich, den angestrebten Vertrag abzuschließen, ohne gleichzeitig die in Punkt 6 der AGB enthaltene Zustimmungserklärung abzugeben. Dieser Umstand ist mit dem Erfordernis der Freiwilligkeit iSd § 4 Z 14 DSG 2000 und § 8 Abs. 1 Z 2 DSG 2000 nicht vereinbar. Dass dem Kunden die Möglichkeit eingeräumt werde, die von ihm zunächst abgegebene Zustimmungserklärung jederzeit wieder zu widerrufen (»Opt-out«), vermag an diesem Ergebnis nichts zu ändern. Die jederzeitige Widerrufbarkeit ist Voraussetzung dafür, dass eine Zustimmungserklärung als Rechtsgrund für die Verwendung von Daten geeignet ist (vgl §§ 8 Abs. 1 Z 2, 9 Abs. 1 Z 6 DSG 2000). Sie ändert aber nichts daran, dass die Erklärung vorher freiwillig abgegeben worden sein muss.

Hier hat der Kunde nur die Wahl, vom Abschluss des Vertrags Abstand zu nehmen oder die Zustimmungserklärung zu erteilen. Dem kommt deshalb beachtliches Gewicht zu, weil es sich bei dieser Zustimmungserklärung um eine Klausel handelt, die nicht im synallagmatischen Zusammenhang mit den vertraglichen Leistungen steht, sondern in Wahrheit mit diesen Leistungen überhaupt nichts zu tun hat. Die gewählte Gestaltung der AGB führt daher zum Ergebnis, dass auch jene Kunden, die nie bereit wären, eine derartige Zustimmung zu erteilen, aber dennoch den Vertrag abschließen wollen, eine entsprechende Zustimmungserklärung zunächst abgeben müssen, um sie erst in weiterer Folge widerrufen zu können. Dieses Ergebnis ist mit der – streng zu beurteilenden – Freiwilligkeit datenschutzrechtlicher Zustimmungserklärungen nicht zu vereinbaren.

Die Datenschutzkommission hält daher eine derartige Einbindung datenschutzrechtlicher Zustimmungserklärungen in AGB für nicht zulässig. Vielmehr muss dem Kunden die Möglichkeit gegeben werden, den angestrebten Vertrag auch ohne die Abgabe der datenschutzrechtlichen Zustimmungserklärung abzugeben (»Opt-in«-Lösung), etwa durch eine Gestaltung der AGB, bei der die Zustimmungserklärung gesondert anzuklicken ist. Es wurden daher entsprechende Empfehlungen erteilt.

b. Video- und Audioaufzeichnungen zur Qualitätssicherung (K213.137/0009-DSK/2012, 23. 11. 2012)

Sachverhalt:

In einer an die Datenschutzkommission gerichteten anonymen Eingabe wurde vorgebracht, in einem Kurunternehmen würden Video- und Audioaufnahmen, durchgeführt durch eine Agentur, zur Mitarbeiterkontrolle eingesetzt werden. Es wurde um Einschreiten der Datenschutzkommission ersucht, welche dies zum Anlass nahm, amtswgig ein Verfahren nach § 30 DSG 2000 (Kontroll- und Ombudsmannverfahren) einzuleiten. Folgender Sachverhalt hat sich ergeben:

Das Kurunternehmen beauftragte eine Agentur, in dem von ihm betriebenen Kurzentrum in regelmäßigen Abständen von ca. zwei Jahren Qualitätschecks durchzuführen. Diese sollen gewährleisten, dass sich die Qualität der angebotenen Dienstleistungen sowie das Service auf höchstem Niveau bewegen. Mindere Qualität erzeuge Schulungsbedarf der betreffenden Mitarbeiter.

2012 fand ein solcher Qualitätscheck statt. In Zuge dessen wurden Mitarbeiter der beauftragten Agentur mit unerkennbaren Kameras an der Kleidung ausgestattet. Während eines mehrtägigen Aufenthalts wurden Bild- und Tonaufzeichnungen jener Mitarbeiter (des Kurunternehmens) angefertigt, mit welchen die Mitarbeiter der Agentur in diesem Zeitraum aus unterschiedlichen Gründen (z. B. Rezeption, Speisebereich etc.) Kontakt hatten. Die Erfassung von betriebsfremden Personen (Gästen, Lieferanten etc.) konnte dabei nicht ausgeschlossen werden (und fand auch tatsächlich statt). Auch Mitschnitte von Telefongesprächen wurden angefertigt. Die so gewonnenen Aufnahmen wurden ausgewertet und dem Kurunternehmen ausgehändigt. Die Aufnahmen werden bis zum nächsten Qualitätscheck in zwei Jahren gespeichert.

Die Kameras sind nicht gekennzeichnet. Eine Information der Mitarbeiter zum einzelnen Qualitätscheck, etwa jenen im Jahr 2012, fand nicht statt.

Die meisten Mitarbeiter haben eine (so bezeichnete) »freiwillige Zustimmungserklärung zu Videoaufnahmen im Zuge eines Qualitätschecks [...]« unterzeichnet. Wann und ob dies, wie behauptet, vor Antritt des Dienstverhältnisses geschehen ist, ergab sich aus der Unterschriftenliste nicht. Die Verweigerung der Zustimmung soll keine tatsächlichen oder rechtlichen Konsequenzen nach sich ziehen.

Rechtliche Würdigung:

Auftraggeber iSd § 4 Z 4 DSG 2000 für die konkrete Datenverwendung und damit verantwortlich für deren Zulässigkeit ist das Kurunternehmen, die beauftragte Agentur war lediglich als Dienstleister iSd § 4 Z 5 DSG 2000 einzustufen.

Für die rechtliche Beurteilung der Zulässigkeit war zunächst entscheidend, ob die gegenständliche Bildverarbeitung unter den Begriff Videoüberwachung in § 50a Abs. 1 DSG 2000 fällt. Danach ist Videoüberwachung die systematische, insb fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt (überwachtes Objekt) oder eine bestimmte Person (überwachte Person) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte.

Die EB zur RV meinen dazu:

»§ 50a Abs. 1 enthält zunächst eine Definition der Videoüberwachung. Dass dies mit ‚systematischer' Erfassung von Ereignissen umschrieben wurde, soll klarstellen, dass durch eine Summe von Verwendungsschritten (vgl § 4 Z 7) das Ergebnis ‚Überwachung' verwirklicht werden soll. Aufnahmen etwa aus rein touristischen oder künstlerischen Beweggründen aber auch Filmen für ausschließlich familiäre oder persönliche Tätigkeiten (vgl § 45, z. B. bei einem Kindergeburtstag) fallen damit nicht darunter, sehr wohl aber auch gezieltes Fotografieren. Überwachtes Objekt oder überwachte Person ist jene Person, Gegenstand oder Ort, auf die sich die systematische Erfassung von Ereignissen intentional richtet. Sofern Videoüberwachungen für ausschließlich persönliche und familiäre Tätigkeiten überhaupt denkbar sind (z. B. Bildüberwachung von Babys), fallen diese nicht unter die Bestimmungen des § 50a. [...]«

Bei der gegenständlichen Bildverarbeitung, zumal sie systematisch erfolgt, handelt es sich daher um Videoüberwachung iSd § 50a Abs. 1 DSG 2000. Die Zulässigkeit dieser Datenverwendung war folglich anhand der Kriterien des § 50a DSG 2000 zu messen. Der Auftraggeber einer Videoüberwachung hat überdies die in den §§ 50b bis 50e DSG 2000 normierten Pflichten einzuhalten.

§ 50a Abs. 5 DSG 2000 verbietet u. a. Videoüberwachung zu Zwecken der Mitarbeiterkontrolle an Arbeitsstätten. Dazu führen die EB aus:

»Ausdrücklich verboten ist auch die gezielte Videoüberwachung zur Kontrolle von Mitarbeiterinnen und Mitarbeitern an Arbeitsstätten, da hier davon ausgegangen werden kann, dass hier auf Grund der Eingriffstiefe stets ein gelinderes Mittel zur Kontrolle von Mitarbeiterinnen und Mitarbeitern gefunden werden kann. Dieses Verbot schließt nicht die Überwachung von Objekten an Arbeitsstätten (Überwachung von Kassenräumen, Überwachung gefährlicher Maschinen zum Schutz der Mitarbeiterinnen und Mitarbeiter) aus, da derartige Überwachungen nicht auf die Leistungskontrolle von Arbeitnehmerinnen und Arbeitnehmern gerichtet sind.«

Das Kurunternehmen gab zwar als Zweck der Videoüberwachung die Überprüfung der Qualität der angebotenen Dienstleistungen sowie des Services an, im Ergebnis handelt es sich jedoch um Leistungskontrolle von Arbeitnehmern, an die auch entsprechende Folgen (Schulungen) geknüpft werden. Qualitätsüberprüfungen sind zwar datenschutzrechtlich nicht grundsätzlich unzulässig, wenn sie im Einzelfall im überwiegenden berechtigten Interesse des Arbeitgebers liegen. Mit der Regelung in § 50a Abs. 5 DSG 2000 erteilt der Gesetzgeber der Verwendung von Videoüberwachung für solche Qualitätsüberprüfungen eine Absage, weil – wie sich aus den EB ergibt – stets ein gelinderes Mittel zur Kontrolle von Mitarbeitern – hier: direkte Beobachtung; schriftliche Beschreibung des Erlebten – gefunden werden kann.

§ 50a Abs. 5 DSG 2000 normiert ein absolutes Verbot für Videoüberwachung, das auch nicht durch die (ausdrückliche) Zustimmung der Betroffenen (iSd § 4 Z 14 iVm § 50a Abs. 3 Z 3 DSG 2000) umgangen werden kann (zumal deren Freiwilligkeit anzuzweifeln wäre). Ausführungen dazu, dass von den Mitarbeitern die Zustimmung zu dieser Art und Weise von Qualitätschecks eingeholt worden sei, vermögen daher die gegenständlichen Videoaufzeichnungen nicht zu rechtfertigen.

Ebenso waren die gleichzeitig mit den Bildaufnahmen angefertigten Tonaufnahmen bzw. die Aufnahmen von Telefonaten als unzulässig einzustufen. Ein derartiger Eingriff ist schon deshalb unverhältnismäßig, weil auch in diesem Fall die direkte Wahrnehmung und die schriftliche Beschreibung des Erlebten das weitaus gelindere Mittel zur Zielerreichung darstellen würde.

Es war daher gem § 30 Abs. 6 DSG 2000 zur Herstellung des rechtmäßigen Zustands die Empfehlung zu erteilen, das Kurunternehmen möge für Zwecke der Überprüfung der Qualität der von ihr angebotenen Dienstleistungen sowie des Services weder Bild- noch Tonaufzeichnungen erstellen bzw. weiterverarbeiten (Frist zur Umsetzung: zwei Wochen).

Fragen der Verletzung von im Zusammenhang mit Videoüberwachung stehenden Pflichten (jedenfalls: Verletzung der Meldepflicht nach § 50c DSG 2000; Verletzung der Kennzeichnungspflicht nach § 50d DSG 2000; auch: unverhältnismäßig lange Aufbewahrungsdauer der Daten, möglicher Verstoß gegen die Löschungspflicht nach § 50b Abs. 2 DSG 2000) waren daher nicht mehr zu behandeln.

c. Empfehlung zur Einhaltung von Datensicherheitsmaßnahmen (K215.018/0003-DSK/2013, 1.2. 2013)

Sachverhalt:

In seiner Eingabe aus August 2012 führte der Einschreiter aus, dass im Zuge des Neueinbaus von Gasleitungen im denkmalgeschützten Haus, in dem er wohnhaft ist, die Gaszählgeräte auf den Gang verlegt würden, sodass der Zählerstand, Verbrauch (ob und wie viel) etc. einem unbegrenzten Kreis von unbekannten Personen (Mieter und Angehörige, Zusteller etc.) zugänglich gemacht werde. Dadurch sehe er sich in seinem Recht auf Datenschutz massiv beeinträchtigt, macht dazu die Hausverwaltung namhaft, die die Umstände in Besprechungen aber ins Lächerliche gezogen hätte.

Die zur Stellungnahme aufgeforderte Hausverwaltung verwies auf den Gaslieferanten, der vorbrachte, für den Montageort des Zählers seien sicherheitstechnische (Richtlinie der ÖVGW; Allgemeine Verteilernetzbedingungen) und gesetzliche Vorgaben sowie die räumliche Situation vor Ort zu berücksichtigen. Ein »massiver Eingriff« in das Recht auf Datenschutz des Einschreiters sei aber nicht gegeben, das Vorliegen personenbezogener Daten werde bezweifelt, die An- bzw. Abwesenheiten in der Wohnung könne man anhand des Zählerstandes nicht eruieren. Der gleiche Sachverhalt sei überdies auch bei anderen Messstellen (Strom, Wasser) gegeben. Sollte der Eingriff in das Recht auf Datenschutz tatsächlich bestehen, werde die Datenschutzkommission ersucht, anzuleiten, zu welchen Maßnahmen Versorgungsunternehmen verpflichtet seien, um den Zugriff auf die genannten Daten durch Dritte zu unterbinden.

Rechtliche Würdigung:

Gem § 4 Z 1 DSG 2000 sind personenbezogene Daten Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Die Gaszählerstände sind daher personenbezogene Daten des Mieters der Wohneinheit, der wie im gegenständlichen Fall in der Regel auch Verbraucher ist, und stehen unter dem Schutz des Grundrechts auf Datenschutz gem § 1 DSG 2000.

Gem § 14 Abs. 1 DSG 2000 sind für alle Organisationseinheiten eines Auftraggebers, die (personenbezogene) Daten verwenden, Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit (ua.) sicherzustellen, dass die Daten Unbefugten nicht zugänglich sind.

Gem § 14 Abs. 2 Z 5 DSG 2000 ist dabei insb, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist, die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln.

Im gegenständlichen Fall werden die Gaszählerstände zur Erfüllung des Vertrages des Verbrauchers mit dem Netzbetreiber bzw. dem Energielieferanten benötigt. Wird, etwa durch den

allgemein zugänglichen Montageort wie hier, Unbefugten ohne jede Beschränkung der Zugriff auf personenbezogene Daten, die dem Grundrecht auf Datenschutz (§ 1 DSG 2000) unterliegen, ermöglicht, wird der Betroffene (Verbraucher) in diesem Grundrecht verletzt.

Etwaige sicherheitstechnische Vorgaben (gesetzliche Vorgaben wurden trotz Behauptung nicht näher angeführt) können einen Eingriff in das Grundrecht auf Datenschutz nicht rechtfertigen.

Es war daher gem § 30 Abs. 6 DSG 2000 zur Herstellung des rechtmäßigen Zustands die Empfehlung zu erteilen, geeignete Datensicherheitsmaßnahmen zu ergreifen, um den Zugriff auf personenbezogene Daten, die im Gaszählgerät gespeichert sind, durch Unbefugte zu unterbinden. Eine Frist von sechs Monaten zur Umsetzung schien in Anbetracht des Umstandes, dass bauliche Veränderungen notwendig sein könnten, angemessen. Die Datenschutzkommission konnte hingegen über diese Empfehlung hinaus entgegen dem Ersuchen keine bestimmten Maßnahmen verpflichtend vorschreiben, um den Zugriff auf die genannten Daten durch Dritte zu unterbinden.

d. Empfehlung zum Personenbezug bei Statistiken (K213.180/0021-DSK/2013, 22.5.2013)

Sachverhalt:

Eine Gebietskrankenkasse übermittelt an interessierte Unternehmen des Bundeslandes mit mehr als 50 Arbeitnehmern auf Anfrage eine Krankheitsgruppen-Statistik der Arbeitnehmer für ein Berichtsjahr.

Diese statistische Auswertung ist so gestaltet, dass in einer Spalte diverse Krankheitsgruppen angeführt sind und daneben, in weiteren Spalten, die Krankenstandsfälle, getrennt nach Männern und Frauen sowie die sich daraus ergebende Gesamtzahl der betroffenen Arbeitnehmer, und die Krankenstandstage, wiederum getrennt nach Männern und Frauen sowie die sich daraus ergebende Gesamtzahl der betroffenen Arbeitnehmer.

Die Übermittlung der Krankheitsgruppen-Statistik stellt eine Maßnahme der betrieblichen Gesundheitsförderung dar.

Die Einschreiterin hatte Bedenken, dass es für den einzelnen Unternehmer im einen oder anderen Fall möglich sei, einen direkten Personenbezug zwischen Diagnose und Mitarbeitern herzustellen, sodass es sich bei den übermittelten Daten nicht bzw. nicht in jedem Fall um indirekt personenbezogene oder anonymisierte Daten handle.

Rechtliche Würdigung:

Die Datenschutzkommission anerkannte das Bemühen der Gebietskrankenkasse, durch die Bereitstellung von Krankheitsgruppen-Statistiken an Betriebe mit mehr als 50 Arbeitnehmern die betriebliche Gesundheitsförderung zu unterstützen und hegte keinen Zweifel, dass dies vom gesetzlichen Auftrag einer Krankenversicherung umfasst ist. Dies hat jedoch im Einklang mit den Bestimmungen des DSG 2000 – insb des Grundrechts auf Datenschutz gemäß § 1 DSG 2000 – zu erfolgen.

Der VfGH hat ausgesprochen, dass auch bei Statistiken – die grundsätzlich nicht personenbezogen sind – sichergestellt sein muss, dass aufgrund der Veröffentlichung keine Rückschlüsse auf (schutzwürdige und durch das Grundrecht auf Datenschutz auch geschützte) Daten gezogen werden können (vgl dazu VfSlg 12.228/1989). Auch § 46 Abs. 1 DSG 2000 sieht eine Privilegierung der Verwendung zulässigerweise für andere Untersuchungen oder auch andere Zwecke ermittelter Daten nur dann vor, wenn die angestrebte wissenschaftliche

Untersuchung oder die Statistik keine personenbezogenen Ergebnisse zum Ziel hat. Dieser Grundsatz war auch auf den vorliegenden Fall anwendbar.

Ist es einem Arbeitgeber aufgrund der übermittelten Krankengruppen-Statistik nämlich möglich, den Bezug zu einem bestimmten Arbeitnehmer herzustellen, so wird der betroffene Arbeitnehmer durch den von seinem Arbeitgeber gezogenen Rückschluss in seinem schutzwürdigen Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten gemäß § 1 Abs. 1 DSG 2000 verletzt. Da es sich bei Gesundheitsdaten gemäß § 4 Z 2 DSG 2000 um sensible Daten handelt, ist diesbezüglich ein besonders strenger Maßstab anzulegen.

Es wurde daher empfohlen, die Krankengruppen-Statistiken so zu gestalten, dass diese für jeden anfragenden Betrieb individuell angepasst wird. Dabei wird auf den Tätigkeitsbereich des Betriebes (bspw Bauwesen, Landwirtschaft etc.) Rücksicht zu nehmen sein, um lediglich jene Krankheitsdaten in die Statistik miteinzubeziehen, die mit der Tätigkeit dieses Betriebes typischerweise verbunden sind. Eine undifferenzierte Übermittlung sämtlicher Krankheitsdaten würde nämlich über das für die betriebliche Gesundheitsförderung erforderliche Maß hinausgehen (vgl dazu nochmals das bereits zitierte Erkenntnis des VfGH, in welchem er ausführte, dass auch die Erhebung von Wirtschaftsdaten auf das Erforderliche und Angemessene beschränkt zu bleiben hat).

Auch wurde empfohlen, eine Trennung in männliche und weibliche Mitarbeiter – und damit einhergehend auch die Ausweisung der für diese Gruppe typischen Krankheiten (wie bspw Krankheiten betreffend der Geschlechtsorgane) – erst dann vorzunehmen, wenn zu einer dieser Gruppen mehr als fünf Personen zu zählen sind. Diese Anzahl scheint nach Ansicht der Datenschutzkommission zu gewährleisten, dass ein Rückschluss auf bestimmte Arbeitnehmer/innen nicht möglich ist.

Zur Umsetzung der Empfehlung wurde eine Frist von zwei Monaten gewährt, weil eine erweiterte Überprüfung der angeforderten Krankheitsgruppen-Statistiken notwendig sein wird.

e. Sozialversicherungsnummer auf Zahlscheinen (K210.714/0016-DSK/2013, 19.7. 2013)

Sachverhalt:

Der Einschreiter fühlt sich dadurch im Recht auf Geheimhaltung personenbezogener Daten verletzt, dass eine Sozialversicherungsanstalt bei der postalischen Vorschreibung eines Behandlungsbeitrages auf dem beigelegten Zahlschein seine Sozialversicherungsnummer (SVNr) aufgedruckt hätte. Die Versicherung führte im Wesentlichen aus, dass die SVNr in der gesamten Korrespondenz mit ihren Kunden und auch im Zahlungsverkehr verwendet werde, um eine eindeutige und verwechslungsfreie Identifikation sicherzustellen. Auf den Vorschreibungen der Behandlungsbeiträge ist auch eine mehrstellige Rechnungsnummer angeführt.

Rechtliche Würdigung:

Die SVNr ist ein personenbezogenes Datum im Sinne des § 4 Z 1 DSG 2000, an der ein Versicherter ein schutzwürdiges Geheimhaltungsinteresse hat. Nach der Rechtsprechung der Datenschutzkommission darf die SVNr nicht als »genereller Identifikator« verwendet werden, dh in Zusammenhängen, die mit sozialversicherungsrechtlichen Sachverhalten nichts zu tun haben; eine solche Verwendung wurde bereits wiederholt als unzulässig bezeichnet. Es wurde hingegen als nicht überschießende Datenverwendung gewertet, die SVNr dort zu verwenden, wo die eindeutige und unverwechselbare Bezeichnung des Betroffenen notwendig ist (vgl den Bescheid vom 25. 2. 2009, GZ K121.422/0002 DSK/2009).

In ähnlicher Weise hat sich auch der gemäß § 41 DSG 2000 beim Bundeskanzleramt eingerichtete Datenschutzrat bereits mehrmals geäußert (vgl dazu bspw die Stellungnahme des Datenschutzrates zur Untersuchung von Alternativen zur SVNr in der Bildungsdokumentation vom 25. 2. 2010, siehe www.bka.gv.at/DocView.axd?CobId=38592).

Vorliegend ist zwar unbestritten ein sozialversicherungsrechtlicher Zusammenhang gegeben, jedoch nur im Verhältnis zwischen dem Versicherten und seiner Sozialversicherung. Wird jedoch die SVNr wie hier auf einem Zahlschein abgedruckt, so wird dieses Datum auch den Bediensteten der die Überweisung durchführenden Bank bekannt. Diesen ist es daher möglich, in Verbindung mit dem auf dem Zahlschein angeführten Namen des Kontoinhabers den Bezug zu diesem herzustellen, weshalb der betroffene Versicherte dadurch in seinem schutzwürdigen Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten gemäß § 1 Abs. 1 DSG 2000 verletzt wird. Dass die Bediensteten einer Bank selbst einer gesetzlichen Verschwiegenheitspflicht unterliegen (vgl § 38 BWG) ändert daran nichts, weil das Bankgeheimnis nur gegenüber Dritten gilt. Der Anspruch auf Geheimhaltung eines Versicherten gilt jedoch auch gegenüber den Bediensteten (s)einer Bank.

Die Datenschutzkommission übersah nicht, dass es angesichts der großen Anzahl der Versicherten zu Zuordnungsproblemen aufgrund von Schreibfehlern kommen kann. Dass dieser Problematik jedoch nur unter Zuhilfenahme der SVNr auf einem Zahlschein wirksam begegnet werden kann – wobei auch hier Schreibfehler nicht ausgeschlossen sind – war nicht nachvollziehbar. Wie der Einschreiter schlüssig geltend macht, ist einer Zahlungsvorschreibung im Regelfall eine Rechnung mit mehrstelliger Rechnungsnummer angeschlossen. Die Rechnungsnummer, die im Übrigen wie auch die SVNr auf einem Zahlschein im Feld »Verwendungszweck« maschinell eingefügt werden könnte, sowie der Name des Versicherten, der ebenfalls maschinell eingefügt wird, sollten eine problemlose Zuordnung ermöglichen. Darüber hinaus ist darauf hinzuweisen, dass im Lichte des sich aus § 1 Abs. 2 und § 7 Abs. 3 DSG 2000 ergebenden Grundsatzes, wonach ein Eingriff in das Grundrecht auf Datenschutz jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden darf, mit der Anführung der SVNr auf der Rechnung, die im Übrigen an den Versicherten selbst adressiert ist und somit vorerst nur von diesem eingesehen werden kann, das Auslangen gefunden werden kann.

Es wurde daher empfohlen, an Stelle der SVNr eine andere, dem Versicherten eindeutig zuordenbare Nummer auf Zahlscheinen zu verwenden. Zur Umsetzung der Empfehlung wurde eine Frist von drei Monaten gewährt, weil eine Neuorganisation der Zahlungszuordnung notwendig sein wird.

f. Verwendung von Bonitätsdaten

Zahlreiche Eingaben betrafen die Verwendung von Bonitätsdaten, oft im Zusammenhang mit Kreditauskunfteien (§ 152 GewO), wobei der Großteil der Fälle sich auf drei bestimmte Kreditauskunfteiunternehmen beschränkte.

Häufig endeten die Fälle mit einer Löschung der Betroffenen aus einer Bonitätsdatenbank, wodurch jedenfalls ein rechtmäßiger Zustand hergestellt war. Sofern es sich nicht überhaupt um Verwechslungen oder Irrtümer handelte, vermochten die Einschreiter häufig Gründe anzugeben, die die Aussagekraft der Daten im Hinblick auf ihre Bonitätslage fragwürdig erscheinen ließen; es musste festgestellt werden, dass etwa die begründeten Bestreitung von als unbezahlt vorgemerkten Forderungen oder sogar eine gerichtliche Entscheidung, aus der sich das Nichtbestehen der Forderung ergab, in dem Kreditinformationssystem nicht entsprechend sichtbar gemacht wurde.

In einigen Fällen erachtete die DSK die Bonitätsdatenspeicherung auch als rechtmäßig. Sowohl Kreditauskunfteien als auch deren Datenlieferanten wurden aber daran erinnert, beim Umgang mit derartigen Daten besondere Sorgfalt walten zu lassen und auf die Datenrichtigkeit zu achten.

Derzeit sind bezüglich des Kreditinformationssektors noch mehrere Verfahren über Eingaben (§ 30 Abs. 1 DSG 2000) sowie auch ein amtswegig eingeleitetes Kotrollverfahren (§ 30 Abs. 3 DSG 2000) anhängig, in denen zum Teil auch die Durchführung einer Einschau vor Ort (§ 30 Abs. 2 DSG 2000) durchgeführt wurde.

g. Videoüberwachung

Eine zahlenmäßig sehr große Gruppe von Eingaben betraf Fragen der Videoüberwachung. Dies betraf die Zulässigkeit von Anlagen an sich, die Abgrenzung der überwachten Örtlichkeit (etwa im nachbarschaftlichen Bereich privater Wohnhäuser), aber auch die Erfüllung von Auftraggeberpflichten, wie der Melde- oder Kennzeichnungspflicht. Vermehrt hatte die Datenschutzkommission dazu das Instrument der Einschau in Datenanwendungen in Anspruch nehmen müssen, um etwa strittige Fragen betreffend Erfassungswinkel und Funktionsweise von Systemen zu klären. In der überwiegenden Zahl der Fälle war dabei – auch in als nicht friktionsfrei zu bezeichnenden Verhältnissen zwischen Einschreiter und Betreiber der Anlage – die Kooperationsbereitschaft der Betreiber äußerst positiv. In einigen Fällen waren Empfehlungen auszusprechen bzw.. wegen Verletzung von Melde- und Kennzeichnungspflicht Verwaltungsstrafanzeigen zu erstatten.

Immer wieder hat die Datenschutzkommission in Verfahren nach § 30 DSG 2000 betreffend Videoüberwachung schwierige Auslegungsfragen betreffend die Zulässigkeit oder die Erfüllung von Auftraggeberpflichten zu lösen. So wurde etwa die Erfassung von Kennzeichen per Kamera zur Einfahrtskontrolle in Garagen als Videoüberwachung iSd § 50a Abs. 1 DSG 2000 gesehen, die nur dann registrierungsfähig ist, wenn eine konkrete Gefährdung durch so genannte gefährliche Angriffe, das sind idR gerichtlich strafbare Vorsatztaten, vorliegt. Die Einfahrtskontrolle auf diese Weise für Zwecke der reinen Besitzstörung ist nicht zulässig. Auch wurde etwa zur Kennzeichnungspflicht festgehalten, dass neben dem Informationsgedanken in der Praxis vom Auftraggeber nicht stets verlangt werden kann, dass die Kennzeichnung jedenfalls ein Ausweichen des überwachten Raumes ermöglichen muss, sondern nur, wo dies tunlich ist (vgl. dazu den Fall der Fassadenüberwachung eines Geschäftslokales mit angrenzendem/r Gehsteig oder Fußgängerzone).

h. Adressdaten

In Verfahren nach § 30 DSG 2000 war es der Datenschutzkommission auch möglich, unkompliziert und rasch die – in vielen Fällen durch den Einschreiter per direkter Korrespondenz bereits versuchten – Löschung von Adressdaten durchzusetzen. Die meist auf Basis einer früheren Zustimmungserklärung oder im Rahmen des Gewerbes des § 151 GewO (Adressverlag) erlangten Daten konnten so vor einer weiteren Verwendung bewahrt werden. In manchen Fällen hat sich hier die – gesetzlich nicht vorgesehene – Sperre gegenüber der physischen Löschung als vorteilhaft für die Betroffenen erwiesen, weil nur so sichergestellt werden konnte, dass der Auftraggeber die Daten auch bei späterer erneuter Ermittlung nicht weiter verwendet.

8.3 Genehmigungsverfahren für internationalen Datenverkehr

Die Auswertung der Genehmigungsverfahren für internationalen Datenverkehr gemäß § 13 DSG 2000 im Berichtszeitraum bekräftigt nur die in früheren Jahren gemachte Beobachtung, dass die Anträge fast ausschließlich von Konzernunternehmen gestellt werden.

Diesem Umstand wurde mit einer neuen Standardanwendung getragen, die einige Datenanwendungen von Konzernen von der Melde- und Genehmigungspflicht ausnimmt (eingefügt mit der Novelle zur StMV 2004, BGBl. II Nr. 306/2012). Es handelt sich dabei um Fälle, die von der Datenschutzkommission in der Vergangenheit problemlos genehmigt wurden und daher die Bedingung für eine Standardanwendung erfüllen, wonach die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich sein muss.

Die neue Standardanwendung SA033 »Datenübermittlung im Konzern« umfasst mehrere Unterpunkte: »Konzernweite Kontakt- und Termindatenbank«, »Karrieredatenbank«, »Verwaltung von Bonus- und Beteiligungsprogrammen eines Konzerns« und »Technische Unterstützung«.

Die Datenschutzkommission hat eine weitere signifikante Entscheidung zu Matrixorganisationen erlassen (Bescheid K178.447/0009-DSK/2012 vom 27. Juni 2012), die neben der im Datenschutzbericht 2011 erwähnten Entscheidung K178.414/0006-DSK/2011 vom 30. September 2011 als Grundlage für die weitere Behandlung von Matrixorganisationen dienen kann. In diesem Fall wurde eine Regelung im Arbeitsvertrag verwendet, um die schutzwürdigen Geheimhaltungsinteressen der Mitarbeiter zu berücksichtigen.

Im Berichtszeitraum zeigte sich deutlicher als je zuvor die Bedeutung des Zusammenhanges zwischen dem Verfahren für eine Genehmigung im internationalen Datenverkehr und dem dazugehörenden Verfahren zur Meldung einer Datenanwendung gemäß § 17 DSG 2000. Die grundsätzliche Zulässigkeit einer Datenanwendung wird im Meldeverfahren geprüft. Ein Antrag auf Genehmigung im internationalen Datenverkehr besteht daher meist aus zwei Verfahren, die koordiniert werden müssen.

Abschließend muss festgestellt werden, dass die Koordination innerhalb der Konzerne ein Problem darstellt, das weder von der Datenschutzkommission, noch von den Tochtergesellschaften in Österreich und ihren Rechtsvertretern hinreichend gelöst werden konnte. Mängel in der Koordination sorgen für sachliche Probleme wie z.B. widersprüchliche Dokumente sowie Probleme beim Verfahrensablauf, die zu aufwendigen Verfahren führen.

8.4 Gesetzlicher Handlungsbedarf

8.4.1 Entlastung des DVR

Wie bereits im vorigen Datenschutzbericht ausgeführt wurde, stellt eines der Hauptprobleme der Datenschutzkommission die permanente Überlastung des DVR dar. In diesem Zusammenhang ist auch zu erwähnen, dass der am 25. Jänner 2012 von der Europäischen Kommission vorgestellte Entwurf einer Datenschutz-Grundverordnung eine generelle Meldepflicht nicht mehr vorsieht, dass aber riskante Datenverwendungen auch weiterhin vorweg von der Datenschutzbehörde geprüft werden sollen. Es scheint daher erwägenswert, im Lichte dieser geplan-

ten Entwicklungen auf EU-Ebene bereits gewisse Entlastungen im Meldewesen vorzusehen. Aus Sicht der Datenschutzkommission ist es unbedingt notwendig, legistisch eine Entlastung des DVR vorzusehen. Da seit September 2012 DVR-Online operativ wurde und die nicht der Vorabkontrolle unterliegenden Meldungen nunmehr ohnehin automatisiert erfolgen, wäre vor allem eine Reduktion der vorabkontrollpflichtigen Datenanwendungen notwendig. Weiters wäre eine Lösung für die Bewältigung der Altlasten anzustreben.

Im Berichtszeitraum wurde vom Bundeskanzleramt der Entwurf einer »DSG-Novelle 2012« versendet, der zu einer Entlastung des DVR im Sinne der oben erwähnten Punkte geführt hätte. Auch eine Rechtshilfeverpflichtung zwischen bestimmten Behörden und der Datenschutzkommission war in diesem Entwurf vorgesehen, welche aus Sicht der Datenschutzkommission ebenso dringend notwendig wäre, da sich Ermittlungen und Vorort-Kontrollen im gesamten Bundesgebiet aufgrund der angespannten personellen Situation praktisch nicht möglich sind. Der Entwurf wurde in der Legislaturperiode, die im Herbst 2013 endete, nicht beschlossen. Daher ist weiterhin eine legistische Lösung zur Entlastung des DVR anzustreben.

8.4.2 Bonitätsinformation

Wie auch im vorhergehenden Berichtszeitraum wurden auch in diesem Berichtszeitraum bei der Datenschutzkommission einige Beschwerden bezüglich der Ermittlung und weiteren Verwendung von Kredit- und Bonitätsinformationen eingebracht. Wie bereits im letzten Datenschutzbericht angesprochen ist die Datenschutzkommission bei der Behandlung dieser Fälle zur Auffassung gelangt, dass in diesem Bereich, in dem nicht ordnungsgemäße Datenverwendung für die Betroffenen auch sehr wichtige wirtschaftliche Implikationen hat, gesetzlicher Handlungsbedarf besteht, soweit die anstehenden Probleme nicht durch Verhaltensregeln gemäß § 6 Abs. 4 DSG 2000 gelöst werden können: Es müssten die §§ 152 der GewO 1994 betr. »Auskunfteien über Kreditverhältnisse« und 118 über »Inkassoinstitute« – ähnlich wie dies bei § 151 GewO hinsichtlich der Adressverlage und Direktmarketingunternehmen geschehen ist – mit genaueren Regelungen über die Zulässigkeit der Ermittlung von Bonitätsdaten, insbesondere über die zulässigen Quellen, über die Pflichten der Auftraggeber zur Qualitätssicherung bei gespeicherten Bonitätsdaten, über die zulässige Speicherdauer und über die effiziente Durchsetzung der Betroffenenrechte, insbesondere Löschungsansprüche, angereichert werden. Der gegenwärtige Zustand ist jedenfalls nach wie vor von großer Rechtsunsicherheit geprägt, was zu den oben erwähnten Beschwerden an die Datenschutzkommission über die Datenverwendung in diesem Bereich geführt hat. Aus Sicht der Datenschutzkommission sollten daher die politischen Bestrebungen, hier eine entsprechende gesetzliche Regelung in Anspruch zu nehmen, (wieder) aufgenommen werden.

8.4.3 Videoüberwachung

Wie bereits in den vorhergegangenen Berichten erachtet es die Datenschutzkommission für notwendig, den Begriff der Videoüberwachung (§ 50a Abs. 1 DSG 2000) zu schärfen. Während nämlich die Materialien zur DSG-Novelle 2010, womit dieser Begriff eingeführt wurde, Einschränkungen bei der Erfüllung des Begriffes sehen, legt der Wortlaut nahe, dass unter Videoüberwachung sämtliche Bildverarbeitung bezogen auf ein Objekt bzw.. eine Person zu verstehen ist, ganz unabhängig vom damit verbundenen Zweck. Da aber dem Gesetzgeber nicht unterstellt werden kann, dass er reine Info-Webcams (Wetter, Disco, Christkindlmarkt etc.), aber auch Kameras, die als Mittel zum Zweck der reinen Zutrittskontrolle eingesetzt werden sollen, oder Kameras zur Produktionskontrolle in derselben Weise regeln wollte, wie Kameras, die zur Abwehr von gefährlichen Angriffen eingesetzt werden, wird angeregt, eine Zweckdefinition in der Begriff aufzunehmen. Konsequenz daraus wäre, dass Kameras, die zu dort nicht genannten Zwecken eingesetzt werden, nach den allgemeinen Regeln der §§ 6ff DSG 2000 zu beurteilen wären und nicht den Regeln des § 50a DSG 2000 unterlägen.

9 Internationale Zusammenarbeit mit anderen unabhängigen Datenschutz-Kontrollstellen

9.1 Allgemeines

Die Internationalen Datenschutzkonferenzen der letzten Jahre Uruguay (2012) und Warschau (2013) haben – wie schon die Konferenzen in den Vorjahren – vor allem die Globalisierung der Grundgedanken des Datenschutzes vorangetrieben. Bei der internationalen Datenschutzkonferenz in Warschau wurden vor allem die Bereiche »Webtracking« und die Angleichung internationaler Datenschutz-Standards diskutiert.

Davon abgesehen stellte im Berichtszeitraum die Arbeit an einem komplett neuen Rechtsrahmen für den Datenschutz auf der Grundlage des Art. 16 AEUV ein die Datenschutzszene beherrschendes Thema dar. Am 25. Jänner 2012 wurden von der Europäischen Kommission der Öffentlichkeit Vorschläge für zwei Datenschutz-Rechtsinstrumente – eine Verordnung für den Bereich der ehemaligen »ersten Säule« und eine Richtlinie für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen präsentiert. Diese Vorschläge wurden im Berichtszeitraum von der Ratsarbeitsgruppe »Datenschutz und Informationsaustausch« und dem Ausschuss für Bürgerrechte des Europäischen Parlaments diskutiert. Während im Rat noch keine Einigung über einen gemeinsamen Standpunkt erfolgte, hat der Ausschuss für Bürgerrechte am 21. Oktober 2013 bereits einen Beschluss zu den beiden geplanten Rechtsinstrumenten gefasst.

Auch der Europarat hat 2010 beschlossen, seine Datenschutzkonvention zu modernisieren und zu überarbeiten. Entsprechende Diskussionen fanden im beratenden Ausschuss (sog. »T-PD«), der rechtlich auf der Konvention selbst basiert, statt. Das T-PD hat seine Arbeit beendet und einen entsprechenden Beschluss gefasst, der nunmehr in einer »Ad hoc- Gruppe« diskutiert wird.

9.2 Zusammenarbeit im Rahmen der Art. 29 Gruppe

Die aus den Vertretern der nationalen Datenschutz-Kontrollstellen (iSd Art. 28 der RL 95/46) zusammengesetzte Art. 29 Gruppe hat ihre Bedeutung für die Weiterentwicklung des europäischen Datenschutzes im Berichtszeitraum nachhaltig unter Beweis gestellt. Technologische Neuheiten ebenso wie neue Business-Konzepte werden dort zuerst auf ihre datenschutzrechtlichen Implikationen hin untersucht und beurteilt.

Die Art. 29 Gruppe wurde wiederholt mit Fragen im Zusammenhang mit den neuen von der EU-Kommission entworfenen Datenschutzinstrumenten befasst.

Es wäre im dringenden nationalen Interesse Österreichs, der Datenschutzbehörde jenes Personal zur Verfügung zu stellen, das notwendig ist, um an den zahlreichen Aufgaben der Art. 29 Gruppe mitzuarbeiten und dadurch den österreichischen Standpunkt in die erarbeiteten Lösungsvorschläge für neuartige Probleme einfließen zu lassen. Auch wenn die Art. 29 Gruppe keine bindenden Entscheidungen erlassen kann, kommt ihren Äußerungen doch wesentliche Bedeutung zu, da diese – auch global – als maßgebliche Interpretationen des europäischen Datenschutzrechtes angesehen werden, an welchen sich nationale Lösungen messen lassen müssen.

Im Berichtszeitraum hat sich die Art. 29 Gruppe insbesondere mit folgenden Themen auseinander gesetzt:

a. Arbeitspapier zu epSOS (WP 189)
b. Stellungnahme zu den Reformvorschlägen im Bereich des Datenschutzes (WP 191)
c. Stellungnahme zur Gesichtserkennung bei Online- und Mobilfunkdienste (WP 192)
d. Stellungnahme zu Entwicklungen im Bereich biometrischer Technologien (WP 193)
e. Stellungnahme zur Ausnahme von Cookies von der Einwilligungspflicht (WP 194)
f. Recommendation on the Standard Application form for Approval of Binding Corporate Rules for t he Transfer of Personal Data for Processing Activities (WP 195a) und Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter (WP 195)
g. Stellungnahme zum Cloud Computing (WP 196)
h. Stellungnahme zum Entwurf des Beschlusses der Kommission über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (Datenschutzrichtlinie für elektronische Kommunikation)(WP 197)
i. Stellungnahme zum Schutzniveau für personenbezogene Daten im Fürstentum Monaco (WP 198)
j. Stellungnahme mit weiteren Beiträgen zur Diskussion der Datenschutzreform (WP 199)
k. Beitrag zu den vorgeschlagenen Durchführungsrechtsakten (WP 200)
l. Stellungnahme mit weiteren Beiträgen zur Diskussion über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (WP 201)
m. Stellungnahme zu Apps auf intelligenten Endgeräten (WP 202
n. opinion on purpose limitation (WP 203), dzt. nur engl. verfügbar
o. Erläuterndes Dokument zu verbindlichen unternehmensinternen Datenschutzregelungen für Auftragsverarbeiter (WP 204)
p. Stellungnahme 4/2013 zum Muster für die Datenschutzfolgenabschätzung (»Muster«) für intelligente Netze und intelligente Messsysteme, erstellt durch die Sachverständigengruppe 2 der Taskforce der Kommission für intelligente Netze (WP 205)
q. Stellungnahme zu intelligenten Grenzen (WP 206)
r. Opinion 06/2013 on open data and public sector information ('PSI') reuse (WP 207)
s. Working Document providing guidance on obtaining consent for cookies (WP 208), dzt. nur englisch verfügbar

Sämtliche zitierten Arbeitspapiere können auf der Homepage der EU-Kommission nachgelesen werden.[17]

In den Unter-Arbeitsgruppen wurden im Berichtszeitraum auch Vorarbeiten zu einigen wichtigen Themen geleistet, wie etwa zur EU-Datenschutzreform, zu zahlreichen technischen Themen wie Cloud computing oder zu biometrische Daten und E-Government. Weitere Untergruppen beschäftigen sich mit dem Datenschutz im Bereich »Polizei und Justiz«, Datenschutz bei finanziellen Transaktionen und der Bewältigung der Globalisierung, etwa mittels verbindlicher unternehmensinterner Richtlinien (Binding Corporate Rules – BCRs) und der Entwicklung von ISO-Standards.

17 Sämtliche veröffentlichte Expertisen der Art. 29 Gruppe (»opinions«) sind auf der Homepage der EU-Kommission unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm einsehbar.

9.2.1 Zu einzelnen Themen von generellem Interesse

9.2.1.1 zur EU-Datenschutzreform

Die Art. 29 Datenschutzgruppe hat sich in einigen Stellungnahmen zu den von der Europäischen Kommission vorgelegten Rechtsinstrumenten geäußert. In WP 191 gibt die Gruppe eine grundsätzliche Stellungnahme zu beiden Vorschlägen ab. Die Gruppe begrüßt grundsätzlich die Vorschläge, die darauf gerichtet sind, die Position der betroffenen Person zu stärken, den für die Verarbeitung Verantwortlichen stärker in die Verantwortung zu nehmen und die Stellung der Aufsichtsbehörden auf nationaler und internationaler Ebene zu verbessern. Bei weiterer Verbesserung könnten die vorgeschlagenen Vorschriften einen deutlichen Abbau der bestehenden rechtlichen Fragmentierung bewirken und den Datenschutz europaweit stärken. Die Datenschutzgruppe begrüßt insbesondere die Aufnahme von Bestimmungen, die dem für die Verarbeitung Verantwortlichen Anreize bieten, von Beginn an in vernünftigen Datenschutz zu investieren (Datenschutz-Folgenabschätzungen, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen). Die Vorschläge weisen den mit der Verarbeitung personenbezogener Daten Befassten während des gesamten Lebenszyklus der Daten eine klare Verantwortung und Rechenschaftspflicht zu. Die Datenschutzgruppe unterstreicht die Bedeutung der Bestimmungen, mit denen – insbesondere durch die Präzisierung des Begriffs »Einwilligung«, die Einführung eines allgemeinen Transparenzgrundsatzes und verbesserte Rechtsschutzmechanismen – die Rechte der betroffenen Person klargestellt und gestärkt werden sollen. Darüber hinaus wird die Einführung einer Meldepflicht für Verletzungen des Schutzes personenbezogener Daten und die damit einhergehende Vereinheitlichung in allen Bereichen sehr positiv eingeschätzt. Die Datenschutzgruppe begrüßt ferner, dass die Vorschläge die Befugnisse und Zuständigkeiten der Aufsichtsbehörden harmonisieren, damit diese sowohl allein als auch gemeinsam die Einhaltung der Vorschriften wirksamer gewährleisten und nötigenfalls durchsetzen können, etwa durch Verhängung hoher Geldbußen. Trotz ihrer grundsätzlich positiven Haltung gegenüber der vorgeschlagenen Verordnung ist die Datenschutzgruppe der Ansicht, dass der Vorschlag in Teilen präzisierungs- und verbesserungsbedürftig ist. Im Hinblick auf die Richtlinie für den Datenschutz im Bereich der Polizei und Justiz zeigt sich die Datenschutzgruppe hingegen von dem mangelnden Ehrgeiz der Kommission enttäuscht und fordert nachdrücklich strengere Vorschriften. Enttäuschend sei auch die Tatsache, dass kein einheitliches Rechtsinstrument für alle Bereiche vorgelegt wurde.

In weiterer Folge enthält das Dokument eine Reihe von Anregungen zu den einzelnen Themenkomplexen, wobei auch auf fehlende Bestimmungen hingewiesen wird.

Als positive Aspekte der Verordnung wird Folgendes festgehalten:

- insgesamt bietet die Verordnung durch präzisere Begriffsbestimmungen und Vorschriften, die auf eine einheitlichere Anwendung der Rechtsvorschriften abzielen und somit den freien Verkehr von Daten erleichtern, mehr Klarheit.
- Die Verordnung stärkt die Rechte natürlicher Personen. Beispiele hierfür sind mehr Transparenz, bessere Kontrolle der Verarbeitung, Datenminimierung, besondere Vorschriften für die Verarbeitung personenbezogener Daten von Kindern, Stärkung des Rechts auf Auskunft über Daten, Stärkung des Widerspruchsrechts, Recht auf Datenportabilität, Stärkung des Rechts auf Löschung von Daten (»Recht auf Vergessenwerden«) und Stärkung des Rechts auf Rechtsschutz durch die Datenschutzbehörden als auch auf gerichtlichen Rechtsschutz.
- Für die für die Verarbeitung Verantwortlichen bringt die Verordnung Vereinfachung und mehr Kohärenz, eine stärkere Fokussierung auf ihre Rechenschaftspflicht für verarbeitete Daten und die Pflicht, dies anhand von Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, Datenschutz-Folgenabschätzungen, durch die Benennung eines Datenschutzbeauftragten, die Einhaltung der Meldepflichten für Verletzungen des Schutzes personenbezogener Daten und ein vorbeugendes Herangehen an grenzüber-

schreitende Datenübermittlungen nachzuweisen. Darüber hinaus werden verbindliche unternehmensinterne Vorschriften ausdrücklich als Instrument zur Handhabung grenzüberschreitender Datenübertragungen anerkannt.
- Es wird eine Rechtsgrundlage für die für Auftragsverarbeiter geltenden Datensicherheitsvorschriften geschaffen. Außerdem werden Auftragsverarbeiter verpflichtet, für bestimmte Verarbeitungsvorgänge die Pflichten des für die Verarbeitung Verantwortlichen zu übernehmen, wenn der Auftragsverarbeiter dabei über die Anweisungen des für die Verarbeitung Verantwortlichen hinausgeht (relevant für Cloud-Anbieter).
- Die Verordnung stärkt die Unabhängigkeit und die Befugnisse von Datenschutzbehörden. Beispiele dafür sind die Befugnis zur Verhängung von Geldbußen, die Pflicht zur Zurateziehung bei legislativen Maßnahmen sowie Bestimmungen zur Gewährleistung einer einheitlichen Anwendung und nötigenfalls Durchsetzung der Rechtsvorschriften, insbesondere durch das Kohärenzverfahren.

Als negativ werden unter anderem die weitgehenden Befugnisse der Europäischen Kommission kritisiert. Dies betrifft sowohl die hohe Zahl der delegierten Rechtakten als auch die Eingriffsbefugnisse im Rahmen des Kohärenzverfahrens.

In einem weiteren Dokument (WP 199) nimmt die Gruppe zu speziellen Themenproblemen, die in der Diskussion in Ratsarbeitsgruppe und Ausschuss für Bürgerrechte im Europäischen Parlament eine gewisse Rolle spielten, Stellung. Dies betrifft etwa den Begriff der personenbezogenen Daten, den Begriff der Einwilligung und vor allem die delegierten Rechtsakte, deren Notwendigkeit in einem Anhang im Einzelnen, Artikel für Artikel, evaluiert wird.

In WP 200 wird zu den einzelnen in Aussicht genommenen Durchführungsrechtsakten Stellung genommen und artikelweise eine Bewertung vorgenommen.

In WP 201 wird noch zu einigen Themenbereichen (z. B. Verwendung von Daten unverdächtiger Personen, Rechte der betroffenen Personen, Datenschutz-Folgeabschätzungen und den Befugnissen der Datenschutzbehörden) der Richtlinie »Polizei und Justiz« Stellung genommen.

9.2.1.2 Gesichtserkennung bei Online- und Mobilfunkdiensten

In den letzten Jahren hat sich die Gesichtserkennungstechnologie sehr schnell verbreitet und ist genauer geworden. Darüber hinaus wurde diese Technologie für die Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung von natürlichen Personen in Online- und Mobilfunkdienste integriert. Die Technologie, die einst Science Fiction war, steht heute sowohl öffentlichen als auch privaten Stellen zur Nutzung zur Verfügung. Beispiele für ihre Verwendung im Bereich der Online- und Mobilfunkdienste umfassen soziale Netzwerke und Smartphones.

In dieser Stellungnahme erwähnt die Datenschutzgruppe einige Beispiele und gibt schließlich einige grundsätzliche Empfehlungen ab:

- Empfehlung 1: Wenn der für die Datenverarbeitung Verantwortliche das Bild direkt […] erhält, muss er sicherstellen, dass die gültige Einwilligung der betroffenen Personen bereits vor der Erfassung vorliegt, und ausreichende Informationen bereitstellen, wenn eine Kamera für die Zwecke der Gesichtserkennung genutzt wird.
- Empfehlung 2: Wenn Einzelpersonen digitale Bilder haben und diese bei Online- oder Mobilfunkdiensten für Zwecke der Gesichtserkennung hochladen, müssen die für die Datenverarbeitung Verantwortlichen sicherstellen, dass die die Bilder hochladenden Personen in die Verarbeitung der Bilder eingewilligt haben, die möglicherweise für Zwecke der Gesichtserkennung durchgeführt wird.

- Empfehlung 3: Wenn für die Datenverarbeitung Verantwortliche digitale Bilder von Personen von Dritten erhalten (z. B. wenn sie diese von einer Website kopieren oder von einem anderen für die Datenverarbeitung Verantwortlichen kaufen), müssen sie die Quelle der Bilder und den Kontext, in dem die Originalbilder erworben und verarbeitet werden, sorgfältig prüfen und auch, ob die betroffenen Personen einer solchen Verarbeitung zugestimmt hatten.
- Empfehlung 4: Die für die Datenverarbeitung Verantwortlichen müssen sicherstellen, dass digitale Bilder und Templates nur für den angegebenen Zweck genutzt werden, für den sie zur Verfügung gestellt wurden. Die für die Datenverarbeitung Verantwortlichen sollten technische Kontrollen einführen, um das Risiko zu reduzieren, dass digitale Bilder durch Dritte für Zwecke weiterverarbeitet werden, für die der Nutzer keine Einwilligung erteilt hat. Sie sollten für die Nutzer auch Werkzeuge bereitstellen, mit denen diese die Sichtbarkeit der von ihnen hochgeladenen Bilder überprüfen können, wenn die Verfügbarkeit für Dritte standardmäßig eingeschränkt ist.
- Empfehlung 5: Die für die Datenverarbeitung Verantwortlichen müssen sicherstellen, dass die Bilder von Personen, die keine registrierten Nutzer des Dienstes sind und die in eine solche Verarbeitung nicht auf eine andere Weise eingewilligt haben, nur soweit verarbeitet werden, wie es im begründeten Interesse des für die Datenverarbeitung Verantwortlichen liegt. Beim ersten Beispiel würde das das Einstellen der Verarbeitung und Löschen aller Daten im Falle des Ergebnisses »keine Übereinstimmung« bedeuten. Sicherheitsverletzung während der Übermittlung Im Fall von Online- und Mobilfunkdiensten ist es wahrscheinlich, dass zwischen dem Erwerb des Bildes und den weiteren Verarbeitungsschritten (z. B. dem Hochladen des Bildes von einer Kamera auf eine Website für die Merkmalsextraktion und den Vergleich) eine Datenübermittlung stattfindet.
- Empfehlung 6: Der für die Datenverarbeitung Verantwortliche muss geeignete Schritte unternehmen, um die Sicherheit der Datenübermittlung sicherzustellen. Dazu können eine Verschlüsselung der Kommunikationskanäle oder des erworbenen Bildes selbst zählen. Sofern möglich, und insbesondere im Bereich der Authentifizierung/Verifizierung, sollte die Verarbeitung vor Ort vorgezogen werden.
- Empfehlung 7: Die für die Datenverarbeitung Verantwortlichen müssen sicherstellen, dass die aus einem digitalen Bild für die Erstellung eines Templates extrahierten Daten nur die Informationen enthalten, die für den angegebenen Zweck erforderlich sind, und so eine weitere Verarbeitung verhüten. Templates sollten nicht zwischen Gesichtserkennungssystemen übertragbar sein. Sicherheitsverletzungen während der Datenaufbewahrung Die Identifizierung und Authentifizierung/Verifizierung erfordern wahrscheinlich die Speicherung des Templates für die Verwendung bei einem späteren Vergleich.
- Empfehlung 8: Der für die Datenverarbeitung Verantwortliche muss überlegen, wo die Daten am besten gespeichert werden. Das kann auch im Gerät des Nutzers oder im System des für die Datenverarbeitung Verantwortlichengeschehen. Der für die Datenverarbeitung Verantwortliche muss geeignete Schritte unternehmen, um die Sicherheit der gespeicherten Daten sicherzustellen. Dazu kann die Verschlüsselung des Templates gehören. Ein unbefugter Zugang zu dem Template oder dem Speicherort sollte nicht möglich sein. Insbesondere im Fall der Gesichtserkennung für Zwecke der Verifizierung können biometrische Verschlüsselungstechniken verwendet werden. Bei diesen Techniken ist der kryptographische Schlüssel direkt an die biometrischen Daten geknüpft und wird nur dann erneut erstellt, wenn das richtige, biometrische Daten einer Person zur Verifizierung vorgelegt wird. Es wird kein Bild oder Template gespeichert (folglich eine Art »nicht verfolgbarer Biometrie«).
- Empfehlung 9: Der für die Datenverarbeitung Verantwortliche sollte den betroffenen Personen geeignete Mechanismen zur Verfügung stellen, damit sie gegebenenfalls ihr Zugangsrecht sowohl auf die Originalbilder als auch auf die im Zusammenhang mit der Gesichtserkennung generierten Templates ausüben können.

9.2.1.3 Entwicklungen im Bereich biometrischer Technologien

Biometrische Systeme nutzen bestimmte individuelle Merkmale einer Person zur Identifikation und/oder Authentifikation dieser Person und stellen insoweit enge Verknüpfungen mit den betroffenen Personen her. Die Daten einer Person können gelöscht oder geändert werden. Manipulationen oder Änderungen der Datenquelle hingegen sind nicht möglich. Biometrische Daten werden erfolgreich und wirksam in der Forschung genutzt; sie sind ein wesentliches Element der Forensik und spielen eine wichtige Rolle bei Systemen zur Zugangskontrolle. Sie können helfen, das Sicherheitsniveau zu erhöhen, und sie können dazu beitragen, Identifikations- und Authentifikationsverfahren zu vereinfachen, zu beschleunigen und bequemer zu gestalten. Früher war diese Technologie teuer und hatte entsprechend nur eingeschränkte Auswirkungen auf die Datenschutzrechte natürlicher Personen. Dies hat sich in den letzten Jahren drastisch geändert. DNA-Analysen beanspruchen heute weniger Zeit und sind für nahezu jedermann erschwinglich. Der technische Fortschritt hat dazu geführt, dass Datenspeicher und Rechenkapazitäten billiger wurden. Infolge dieser Entwicklung sind Online-Fotoalben und soziale Netzwerke entstanden, in denen Milliarden von Fotos verwaltet werden. Fingerabdruck-Lesegeräte und Systeme zur Videoüberwachung sind bezahlbare technische Hilfsmittel geworden. Die Entwicklung dieser Technologien hat dazu beigetragen, dass viele Verfahren vereinfacht wurden, zahlreiche Verbrechen aufgeklärt werden konnten und Zugangskontrollsysteme zuverlässiger geworden sind. Diese Entwicklung hat allerdings auch neue Bedrohungen der Grundrechte mit sich gebracht. Die genetische Diskriminierung hat sich zu einem echten Problem entwickelt, und der Diebstahl von Identitäten ist nicht mehr nur eine theoretische Gefahr. Bei anderen neuen Technologien, die auf große Bevölkerungsgruppen abzielen, und die in jüngster Zeit Anlass zu datenschutzrechtlichen Bedenken gegeben haben, steht die Verknüpfung mit bestimmten Personen nicht unbedingt im Vordergrund bzw.. ist diese Verknüpfung mit beträchtlichem Aufwand verbunden. Biometrische Daten hingegen sind direkt mit einer einzigen Person verknüpft. Dies ist nicht immer vorteilhaft, sondern birgt auch erhebliche Nachteile. Die Ausrüstung von Videoüberwachungssystemen und Smartphones mit Funktionen zur Gesichtserkennung, die auf der Nutzung der Datenbanken sozialer Netzwerke beruhen, könnte jegliche Anonymität zunichtemachen und zur Folge haben, dass Einzelpersonen auf Schritt und Tritt überwacht werden. Allerdings könnten Fingerabdruck-Lesegeräte, Geräte zur Erkennung von Venenstrukturen (»Venenscanner«) oder auch einfach ein Lächeln in eine Kamera Chipkarten, Codes, Kennwörter und Unterschriften ersetzen. Diese Zusammenhänge sowie weitere neue Entwicklungen sind Gegenstand dieser Stellungnahme. Ziel dieser Stellungnahme ist es, sowohl die betreffenden Personen als auch die gesetzgebenden Institutionen zu sensibilisieren. Die technischen Innovationen, die allzu häufig nur in ihrer Eigenschaft als Technologien dargestellt werden, die das Erscheinungsbild und die Bedienungsfreundlichkeit von Anwendungen verbessern, könnten auch zu einem schrittweisen Verlust der Privatsphäre führen, wenn keine angemessenen Garantien vorgesehen werden. Daher werden in dieser Stellungnahme technische (wie die Verwendung biometrischer Templates, Speicherung auf einem persönlichen Gerät im Vergleich zu einer zentralen Speicherung, Möglichkeit der Erneuerung des Widerrufs, Verschlüsselung, Schutz gegen Spoofing, automatisierte Mechanismen zur Löschung von Daten) und organisatorische Maßnahmen (z. B. klare Verfahren, detaillierte Regelung bezüglich der Kontrolle von Dienstleistern) erläutert, die die Gefahren im Hinblick auf den Datenschutz und die Verletzung der Privatsphäre verringern und dazu beitragen könnten, Beeinträchtigungen der Privatsphäre und des Grundrechts der bezogenen Daten zu verhindern.

9.2.1.4 Cloud Computing

In dieser Stellungnahme analysiert die Art. 29 Datenschutzgruppe relevante Fragen, die im Europäischen Wirtschaftsraum (EWR) tätige Cloud Computing-Diensteanbieter und ihre Kunden betreffen. Dabei werden alle einschlägigen anzuwendenden Grundsätze aus der EU-Datenschutzrichtlinie (95/46/EG) und der Datenschutzrichtlinie für elektronische Kommunikation

2002/58/EG (in der durch die Richtlinie 2009/136/EG geänderten Fassung) aufgeführt. Trotz der anerkannten wirtschaftlichen und gesellschaftlichen Vorteile des Cloud Computing zeigt die vorliegende Stellungnahme, wie die weit verbreitete Nutzung von Diensten des Cloud Computing zu einer Reihe von Datenschutzrisiken führen kann. Hier geht es in erster Linie um die fehlende Kontrolle über personenbezogene Daten und über unzureichende Informationen darüber, wie, wo und durch wen die Daten verarbeitet bzw.. im Unterauftrag verarbeitet werden. Diese Risiken müssen von öffentlichen Einrichtungen und Privatunternehmen sorgfältig bewertet werden, wenn sie in Betracht ziehen, die Dienste eines Cloud-Anbieters in Anspruch zu nehmen. Die vorliegende Stellungnahme untersucht Fragen, die mit der gemeinsamen Nutzung von Ressourcen mit anderen Parteien verbunden sind; die fehlende Transparenz in einer Outsourcing-Kette, die aus zahlreichen Auftragsverarbeitern und Unterauftragnehmern besteht; das Fehlen eines gemeinsamen, weltweiten Rahmens für die Datenportabilität und die Ungewissheit bezüglich der Zulässigkeit der Übermittlung personenbezogener Daten an Cloud-Anbieter, die außerhalb des EWR niedergelassen sind. Ähnlich wird in der Stellungnahme hervorgehoben, dass der Mangel an Transparenz in Bezug auf die Informationen, die ein für die Verarbeitung Verantwortlicher der betroffenen Person über die Art der Verarbeitung ihrer personenbezogenen Daten geben kann, Anlass zu ernster Besorgnis ist. Die betroffenen Personen müssen darüber informiert werden, wer ihre Daten für welche Zwecke verarbeitet, damit sie ihre diesbezüglichen Rechte ausüben können. Eine wichtige Schlussfolgerung dieser Stellungnahme ist, dass Unternehmen und Verwaltungen, die Cloud Computing nutzen wollen, als ersten Schritt eine umfassende und gründliche Risikoanalyse durchführen sollten. Alle Cloud-Anbieter, die Dienste im EWR anbieten, sollten dem Cloud-Anwender alle Informationen geben, die dieser benötigt, um die Vor- und Nachteile der Inanspruchnahme eines solchen Dienstes gründlich gegeneinander abwägen zu können. Beim Anbieten von Diensten des Cloud Computing sollten Sicherheit, Transparenz und Rechtssicherheit für die Anwender die wichtigsten Aspekte sein. In den Empfehlungen dieser Stellungnahme wird die Verantwortung eines Cloud-Anwenders als für die Verarbeitung Verantwortlicher hervorgehoben, und es wird folglich empfohlen, dass der Anwender einen Cloud-Anbieter auswählt, der die Einhaltung der EU-Datenschutzbestimmungen gewährleistet. In der Stellungnahme werden geeignete vertragliche Absicherungsklauseln angesprochen. Dabei wird gefordert, dass jeder Vertrag zwischen dem Cloud-Anwender und dem Cloud-Anbieter ausreichende Garantien in Bezug auf technische und organisatorische Maßnahmen enthält. Die Empfehlung, dass der Cloud-Anwender überprüfen sollte, ob der Cloud-Anbieter die Rechtmäßigkeit jeder grenzüberschreitenden Datenübermittlung garantieren kann, ist ebenfalls von Bedeutung. Wie bei jedem Entwicklungsprozess stellt auch der Aufstieg des Cloud Computing zu einem weltweiten technologischen Paradigma eine Herausforderung dar. Für sich betrachtet, kann diese Stellungnahme als wichtiger Schritt zur Festlegung der Aufgaben angesehen werden, die von der Datenschutzgemeinde in den folgenden Jahren übernommen werden müssen.

9.2.1.5 Stellungnahme zur Zweckbegrenzung

Diese Stellungnahme analysiert das Prinzip der Zweckbegrenzung. Sie gibt Leitlinien für die praktische Anwendung des Prinzips und des derzeit geltenden Rechtsrahmens und gibt Policy-Empfehlungen für die Zukunft. Die Zweckbindung schützt Betroffene, indem den für die Verarbeitung Verantwortlichen Grenzen für die Datenverwendungen gesetzt werden. Das Konzept der Zweckbindung besteht aus zwei Grundelementen: Personenbezogene Daten dürfen nur für festgelegte eindeutige und rechtmäßige Zwecke ermittelt werden (Zweckbindung) und nicht in mit diesen Zwecken unvereinbarer Weise weiterverarbeitet werden. Die Weiterverarbeitung zu einem anderen Zweck bedeutet nicht unbedingt, dass dieser unvereinbar ist; die Kompatibilität muss von Fall zu Fall beurteilt werden. Eine substantiierte Vereinbarkeits-Bewertung erfordert eine Beurteilung aller relevanten Umstände, insbesondere sollten folgende wichtige Faktoren berücksichtigt werden:

- Das Verhältnis zwischen dem Zweck, für den die Daten ursprünglich ermittelt wurden und dem Zweck der Weiterverarbeitung;
- dem Kontext, in dem die personenbezogenen Daten ermittelt wurden und die angemessenen Erwartungen der Betroffenen im Hinblick auf ihre weitere Verwendung;
- die Art der personenbezogenen Daten und die Auswirkungen der Weiterverarbeitung auf den Betroffenen
- die Schutzmaßnahmen, die der für die Verarbeitung Verantwortliche ergriffen hat, um eine faire Verarbeitung zu gewährleisten und unverhältnismäßige Auswirkungen auf den Betroffenen zu vermeiden.

Die Verarbeitung personenbezogener Daten in einer mit dem ursprünglichen Ermittlungszweck unvereinbaren Weise verstößt gegen das Gesetz und ist daher verboten. Der für die Verarbeitung Verantwortliche kann nicht inkompatible Verarbeitungen legitimieren, indem er die Verarbeitung einfach auf eine neue rechtliche Grundlage in Artikel 7 stützt. Die Zweckbindung kann grundsätzlich nur unter den in Artikel 13 der Richtlinie genannten Bedingungen eingeschränkt werden. Diese Analyse hat auch Konsequenzen für die Zukunft. Artikel 6 Abs. 4 der vorgeschlagenen Datenschutz-Grundverordnung sieht eine weite Ausnahme von dem Erfordernis der Vereinbarkeit vor, die diesen Grundsatz. stark einschränken würde. Die Art.29 Datenschutzgruppe empfiehlt daher, dass der vorgeschlagene Absatz 4 gestrichen wird. Um die Rechtssicherheit zu stärken, empfiehlt die Datenschutzgruppe, dass der Gesetzgeber die oben aufgeführte Liste relevanter Faktoren zur Beurteilung der Kompatibilität in den Rechtsakt aufnehmen soll.

9.2.1.6 Smart Borders

Am 28. Februar 2013 legte die Kommission Vorschläge für ein Einreise-/Ausreisesystem (EES) und ein Registrierungsprogramm für Reisende (RTP) für den Schengen-Raum vor, die zusammen als Vorschläge für »intelligente Grenzen« bezeichnet werden. Außerdem wurde ein Vorschlag für erforderliche Änderungen des Schengener Grenzkodex vorgelegt. Der Vorschlag für ein Einreise-/Ausreisesystem umfasst ein System zur zentrale n Speicherung der Ein- und Ausreisedaten von Drittstaatsangehörigen, die für Kurzaufenthalte im Schengen-Raum zugelassen sind, unabhängig davon, ob sie einer Visumpflicht für ein Schengen-Visum unterliegen. Anstatt die Reisepässe bei der Einreise in den Schengen-Raum und der Ausreise aus dem Schengen-Raum abzustempeln, werden Daten über die Identität des Besuchers sowie über Dauer und Zweck des Aufenthalts bei der Einreise in das System eingegeben und bei der Ausreise überprüft, um sicherzustellen, dass der Drittstaatsangehörige die höchstens zulässige Aufenthaltsdauer nicht überschritten hat. Da das EES ein zentrales System darstellt, ist bei der Prüfung der EES-Daten unerheblich, über welche Grenzübergangsstelle der Drittstaatsangehörige aus dem Schengen-Raum ausreist. In erster Linie soll mit dem System verhindert werden, dass Drittstaatsangehörige, die ursprünglich mit einem gültigen Visum oder für einen zulässigen Zweck für einen Kurzaufenthalt (maximal 90 Tage innerhalb eines Zeitraums von 180 Tagen) eingereist sind, die zulässige Aufenthaltsdauer im Schengen-Raum überziehen. Der Vorschlag für ein EES umfasst ein System, in dem zunächst personenbezogene Daten erfasst werden, die zur Identifizierung von Personen benötigt werden. Diese Daten werden im Wortlaut des Vorschlags nur als »alphanumerische Daten« bezeichnet. Nach drei Jahren sollen auch »biometrische Daten« erfasst werden. Nach zwei Jahren soll geklärt werden, ob Strafverfolgungsbehörden und Drittstaaten Zugang zu den im System gespeicherten Informationen erhalten sollten. Der Vorschlag für ein Registrierungsprogramm für Reisende (RTP) umfasst ein Programm zur Registrierung von Reisenden, die häufig in den Schengen-Raum einreisen (Vielreisende), beispielsweise Geschäftsreisende. Drittstaatsangehörige können den Status als registrierte Vielreisende beantragen, um die Grenzabfertigung zu beschleunigen. Grundlage des RTP bilden ein Zentralregistermit biometrischen Daten sowie ein an die Reisenden ausge-

händigtes »Token«, auf dem eine individuelle Kennnummer gespeichert ist. Die Art. 29 Datenschutzgruppe wiederholt die Bedenken, die sie bereits bei Veröffentlichung der Mitteilung über intelligente Grenzen in ihrem Schreiben an Kommissarin Malmström geäußert hat. Die Datenschutzgruppe hat hinsichtlich der Vorschläge aus datenschutzrechtlicher Sicht unverändert Vorbehalte. Insbesondere hat die Datenschutzgruppe ernsthafte Zweifel daran, dass das Einreise-/Ausreisesystem den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit entspricht und dass die Beeinträchtigungen des Rechtsauf den Schutz personenbezogener Daten gemäß Artikel8 der EU-Charta der Grundrechte gerechtfertigt sind. Diese Stellungnahme konzentriert sich hauptsächlich auf das Einreise-/Ausreisesystem und geht darüber hinaus auf einige spezifische Datenschutzbelange des Registrierungsprogramms für Reisende ein. Hauptziel der Stellungnahme ist die Untersuchung des Einreise-/Ausreisesystems unter dem Aspekt der Notwendigkeit und der Verhältnismäßigkeit und die entsprechende Möglichkeit der Rechtfertigung einer Verletzung der Privatsphäre. Im zweiten Teil der Stellungnahme werden einige spezifische Datenschutzbelange beider Vorschläge behandelt.

9.3 Sonstige Zusammenarbeit auf EU-Ebene

9.3.1 Europol

Europol ist das Europäische Polizeiamt, das EU-weit operiert und schwerwiegende Formen internationaler Kriminalität bekämpfen soll. Dazu werden große Mengen an personenbezogenen Daten verarbeitet, die auf Grund der Zielsetzung von Europol von besonderer datenschutzrechtlicher Bedeutung sind. Aus diesem Grund sind im Europol-Beschluss, mit dem Europol eigene Rechtspersönlichkeit zuerkannt wurde, besondere Rechte der Betroffenen vorgesehen (z. B. Art. 30 – Auskunftsanspruch; Art. 31 – Berichtigung und Löschung von Daten).

Neben den nationalen Kontrollinstanzen (Art. 33), im Wesentlichen die nationalen Datenschutzbehörden, wurde eine Gemeinsame Kontrollinstanz (GKI; »Europol Joint Supervisory Body«)[18] eingesetzt (Art. 34), deren Aufgabe darin besteht, die Tätigkeit von Europol nach Maßgabe des Europol-Beschlusses daraufhin zu überprüfen, ob durch die Verwendung der bei Europol vorhandenen personenbezogenen Daten die Datenschutzrechte von Personen verletzt werden. Die GKI ist auch zuständig für die Prüfung von Anwendungs- und Auslegungsfragen im Zusammenhang mit der Tätigkeit von Europol bei der Verwendung personenbezogener Daten. Weiters führt die GKI jährlich Inspektionen bei Europol durch, weitere Inspektionen zu Sonderfragen sind ebenfalls möglich.

Die österreichischen Mitglieder der GKI werden von der DSK entsandt. Überdies stellt die DSK ein Mitglied der Europol-Inspektionsgruppe, welche im März 2012 und im März 2013 Inspektionen bei Europol durchgeführt hat. Im Jahr 2011 lag der Schwerpunkt der Kontrolle neben der Funktionsfähigkeit des Europol Informations Systems (EIS) (Art. 11ff) und der Rechtskonformität der verarbeiteten Daten in Analytical Work Files (AWF) – Arbeitsdateien (Art. 14) auf dem Schutz von personenbezogenen Daten der Mitarbeiter von Europol. Überdies wurde die Sicherheitseinrichtungen beim neuen Sitz von Europol näher begutachtet. Das Inspektionsteam erstellt einen Bericht, der – nachdem Europol die Möglichkeit zur Stellungnahme eingeräumt wurde und er in der GKI formell verabschiedet wurde – auch veröffentlicht wird. Der Bericht für das Jahr 2013 ist noch nicht angenommen.

18 Die GKI verfügt über eine eigene Website: http://europoljsb.consilium.europa.eu/. Europol selbst ist unter http://www.europol.europa.eu/ zu finden.

Schwerpunkte der Sitzungsarbeit in der GKI Europol im Berichtszeitraum waren die Begutachtung von Verträgen, die Europol hinsichtlich des Datenaustausches mit Drittstaaten abgeschlossen hat, die Begutachtung der geplanten neuen Europol-Verordnung, eine (weitere) Inspektion der Verwendung von Daten im Rahmen des TFTP-Abkommens (US-Terrorist Finance Tracking Program), ein neues Konzept bei der Ausgestaltung der AWF (Orientierung an räumlichen Kriterien anstatt Typen von Verbrechen – damit verbunden eine starke Reduzierung der Zahl der AWF und Eröffnung von Target Groups und Focal Points innerhalb eines AWF) sowie Richtlinien und Bedingungen, die die nationalen Einheiten bei Europol (die Verbindungsbeamten) zu erfüllen haben,

Im Beschwerdeausschuss Europol, der für die Behandlung der Beschwerden von Betroffenen betreffend die Datenverwendung durch Europol zuständig ist, wurden zwischen Jänner 2012 und Dezember 2013 die bereits zuvor anhängig gemachten zwei Beschwerdefälle erledigt.

9.3.2 Schengen

Seit 9. April 2013 ist das Schengener Informationssystem (nach einigen Verzögerungen) der 2. Generation (kurz: SIS II) in Betrieb gegangen. Es löst das Schenger Informationssystem I (kurz: SIS I) sowie das Übergangssystem SIS I+4all ab, die für den Betrieb der nunmehrigen Anzahl von Vertragsstaaten nicht mehr ausreichend dimensioniert waren.

Auch das SIS II ist ein Informationssystem, das Ausschreibungen zu Personen und Sachen enthält. Eine Ausschreibung ist ein in das SIS II eingegebener Datensatz, der den zuständigen Behörden die Identifizierung einer Person im Hinblick auf die Ergreifung spezifischer Maßnahmen ermöglicht. Es wird von Grenzschutzbeamten, Zollbeamten, Visa- und Strafverfolgungsbehörden im Schengen-Raum genutzt und soll ein hohes Maß an Sicherheit gewährleisten.

Das SIS II besteht aus einem zentralen System (dem »zentralen SIS II«); einem nationalen System (»N.SIS II«) in jedem Mitgliedstaat (dem nationalen, mit dem zentralen SIS II kommunizierenden Datensystem); und einer Kommunikationsinfrastruktur zwischen dem zentralen System und den nationalen Systemen, die ein verschlüsseltes virtuelles Netz speziell für SIS-II-Daten und den Austausch von Daten zwischen den für den Austausch aller Zusatzinformationen zuständigen Behörden (SIRENE-Büros) zur Verfügung stellt.

Für das nationale System ist das Bundesministerium für Inneres (BMI) verantwortlich, das zentrale System und die Kommunikationsinfrastruktur wird von der Europäischen Kommission (inhaltlich) sowie von der neu gegründeten EU Agentur für große IT Systeme (EU-Lisa; technisch) betrieben.

Die DSK ist nationale Kontrollinstanz im Sinne des Art.44 der Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS-II-Verordnung), die das Schengener Durchführungsübereinkommen von 1990 (SDÜ) ablöst.

Mit Inkrafttreten des SIS II ist auch die Gemeinsame Kontrollinstanz von Schengen19 aufgelöst worden und durch eine koordinierte Aufsicht durch die nationalen Kontrollinstanzen gemeinsam mit dem Europäischen Datenschutzbeauftragten (EDPS) ersetzt worden. Je nach

19 Die Gemeinsame Kontrollinstanz von Schengen führte eine eigene Website: http://schengen.consilium.europa.eu/. Die Jahresberichte der GKI Schengen sind auf der Website der Datenschutzkommission http://www.dsb.gv.at/ veröffentlicht.

Gegenstand der Kontrolle (nationales oder zentrales System bzw.. Kommunikationsinfrastruktur) ist entweder der EDPS oder sind die nationalen Behörden zur Kontrolle kompetent (vgl. Art. 46 SIS-II-Verordnung).

Das BMI als für die Führung des nationalen Systems zuständiger Auftraggeber trifft auch die Pflicht zur Auskunftserteilung gemäß §§ 1 und 26 DSG 2000 an Betroffene. Fälschlicherweise an die Datenschutzkommission gerichtete Auskunftsbegehren werden daher (weiterhin) an das BMI weitergeleitet. Außerdem lässt sich auf der Website der DSK schon seit Jahren ein Formular (mit englischer Übersetzung) für die Auskunft aus dem SIS II abrufen (http://www.dsb.gv.at/site/6226/default.aspx).

Im Berichtszeitraum wurden folgende Kontrollschwerpunkte gesetzt:

- Prüfung der Ausschreibungen nach Art. 95 SDÜ (Ausschreibung von Personen zur Festnahme und Auslieferung).
- Inspektion des zentralen SIS (I+4all) im Jahr 2012.
- Rechtsfragen im Zusammenhang mit dem Zugang von Europol zu Daten im SIS (II).
- Prüfung der Migration der Daten von SIS I+4all nach SIS II.
- Implementierung von Art. 102A SDÜ.
- Durchführung einer Prüfung zu Fragen der Geltendmachung des Rechts auf Auskunft betreffend Daten im SIS in der Praxis.
- Einsatz einer Arbeitsgruppe von Sicherheitsexperten zur Untersuchung eines Hackerangriffs auf das nationale System von Dänemark.

9.3.3 Zoll

Auf der Basis der Verordnung (EG) 515/97 des Rates über die gegenseitige Amtshilfe zwischen Verwaltungsbehörden der Mitgliedstaaten und die Zusammenarbeit dieser Behörden mit der Kommission im Hinblick auf die ordnungsgemäße Anwendung der Zoll- und Agrarregelung vom 13. März 1997 (ABl. L 82 vom 22. März 1997, S. 1) für den Bereich der ehemaligen 1. Säule der EU sowie des Übereinkommens aufgrund von Artikel K.3 des Vertrages über die Europäische Union über den Einsatz der Informationstechnologie im Zollbereich vom 26. Juli 1995 (ABl. C 316 vom 27. November 1995, S. 34) für den Bereich der ehemaligen 3. Säule der EU wurde ein gemeinsames Zollinformationssystem (ZIS) eingerichtet. Dieses erlaubt es, sowohl in einer Datenbank für den Bereich der gemeinschaftsrechtlichen Zuständigkeiten wie auch in einer Datenbank, die den nicht harmonisierten Bereiche betrifft, Daten über Waren oder Transportmittel sowie über natürliche und juristische Personen zu speichern, für die es tatsächliche Anhaltspunkte gibt, dass sie im Zusammenhang mit Handlungen stehen, die der Zoll- oder der Agrarregelung zuwiderlaufen.

Die Verordnung (EG) 515/97 wurde durch die Verordnung (EG) 766/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die gegenseitige Amtshilfe zwischen Verwaltungsbehörden der Mitgliedstaaten und die Zusammenarbeit dieser Behörden mit der Kommission im Hinblick auf die ordnungsgemäße Anwendung der Zoll- und der Agrarregelung geändert.

Das ZIS ist als Ausschreibungsdatei im Rahmen der Betrugsbekämpfung konstruiert und ermöglicht es jenem Mitgliedstaat, der die Daten in das System eingegeben hat, einem ZIS-Partner in einem anderen Mitgliedstaat zur Durchführung u. a. gezielter Kontrollen zu übermitteln.

Um eine adäquate datenschutzrechtliche Kontrolle zu gewährleisten, wurde durch das vorstehend zitierte Übereinkommen vom 26. Juli 1995 eine gemeinsame Aufsichtsbehörde (Gemeinsame Kontrollinstanz für das ZIS) eingerichtet, für die jedes EU-Mitgliedsland zwei Vertreter

namhaft macht, die von der jeweiligen nationalen unabhängigen Datenschutzbehörde nominiert werden.

Schwerpunkte des Berichtszeitraumes waren die Untersuchung der Anwendung des Rahmenbeschlusses für den Datenschutz auf das ZIS, die Weiterführung einer bereits 2011 initiierten Inspektion des zentralen ZIS, eine Evaluierung des FIDE-Handbuchs sowie die Gestaltung einer Broschüre zur Geltendmachung der Datenschutzrechte im Zusammenhang mit dem ZIS.

Die Verordnung (EG) 766/2008 richtete durch ihren Art. 37 eine Form der koordinierten Kontrolle durch die nationalen ZIS-Aufsichtsbehörden und den Europäischen Datenschutzbeauftragten ein. Die so geschaffene Koordinationsgruppe ZIS nahm ihre Arbeit im März 2010 auf.

Neben der Zusammenarbeit mit der GKI ZIS, die weitgehend dieselben Themenbereiche abzudecken hat (dort eben für den Bereich der ehemaligen 3. Säule der EU), sind im Berichtszeitraum folgende Schwerpunkte in der Tätigkeit gesetzt worden: Information über Entwicklungen im Zollbereich (ua. ist geplant, diesen rechtlich doch sehr zersplitterten Bereich in einem Rechtsakt zu regeln), Vorabkontrolle von Datenanwendungen bei OLAF (Europäisches Amt für Betrugsbekämpfung), Überprüfung der Gruppen von Behörden, die Zugang zu ZIS und FIDE haben, sowie ein Arbeitspapier zu den Rechten der Betroffenen im Bereich Zoll.

9.3.4 Eurodac

Das »Eurodac«-System ermöglicht den Mitgliedstaaten, Asylbewerber sowie Personen zu identifizieren, die beim illegalen Überschreiten einer EU-Außengrenze aufgegriffen wurden. Anhand des Vergleichs der Fingerabdrücke kann ein Mitgliedstaat feststellen, ob ein Asylwerber oder ein Ausländer, der sich illegal in seinem Hoheitsgebiet aufhält, bereits in einem anderen Mitgliedstaat Asyl beantragt hat oder ob ein Asylbewerber illegal in die EU eingereist ist.

»Eurodac« besteht aus einer von der Kommission verwalteten Zentraleinheit, einer computergestützten Datenbank für Fingerabdrücke und elektronischen Einrichtungen für die Datenübertragung zwischen den Mitgliedstaaten und der zentralen Datenbank. Neben den Fingerabdrücken umfassen die von den Mitgliedstaaten übermittelten Daten u. a. den Herkunftsmitgliedstaat, Ort und Zeitpunkt der Antragstellung, das Geschlecht sowie die Kennnummer (Namen werden in diesem System nicht gespeichert, es handelt sich daher um eine Sammlung von »indirekt personenbezogenen Daten« im Sinne des DSG 2000).

Seit 2013 wird Eurodac von EU-Lisa (EU-Agengy for large-scale IT-Systems) geführt.

Im Berichtszeitraum hat sich die zur Kontrolle des Systems eingerichtete Koordinierungsgruppe, bestehend aus Vertretern der nationalen DSB und des Europäischen Datenschutzbeauftragten, mit einem Entwurf einer Verordnung für Eurodac, einer Untersuchung zu unlesbaren Fingerabdrücken sowie einem Security Audit auf nationaler Ebene auseinandergesetzt. Die DSK hat, wie auch in den letzten Berichten an dieser Stelle ausgeführt, bis dato keine Beschwerde oder Anfrage zu Eurodac erhalten.

9.3.5 Visa Information System

Das Visa-Informationssystem (VIS) ist ein System zum Austausch von Daten über Kurzzeit-Visa zwischen den Mitgliedstaaten des Schengenraums. Am 11. Oktober 2011 nahm das System seinen Betrieb auf.

Es besteht ähnlich dem SIS II aus einer zentralen Datenbank, einer nationalen Schnittstelle in den Schengen-Staaten und einer Infrastruktur zur Kommunikation zwischen beiden. Durch die

nationalen Schnittstellen werden Daten zu allen im Schengen-Staat durchgeführten Anträgen, Ausstellungen, Ablehnungen, Annullierungen, Widerrufen und Verlängerungen von Visa durch die zuständigen Autoritäten in das System eingespeist.

Das VIS besteht aus einer zentralen Datenbank, welche eine alphanumerische Suchfunktion besitzt, sowie einem automatisierten System zur Identifizierung von Fingerabdrücken (AFIS), welches neue und bereits in der Datenbank aufgenommene Fingerabdrücke vergleicht.

Der nationale Teil des VIS wird vom BMI, der zentrale Teil und die Kommunikationsinfrastruktur wird (technisch) von EU-Lisa betrieben.

Die Kontrolle von VIS wird ähnlich wie bei SIS II durch die nationalen Datenschutzbehörden gemeinsam mit dem EDPS ausgeübt. Seit November 2012 wurden folgende Themen behandelt: Transfer der Daten zu EU-Lisa; Inspektion der zentralen Datenbank; Austausch von nationalen Erfahrungen in der Kontrolle; Beschluss eines mehrjährigen Arbeitsprogrammes; Diskussion über das auf Subunternehmer, die das VIS in einzelnen ausländischen Vertretungen betreiben, anwendbare Recht.

10 Das Datenverarbeitungsregister

10.1 Allgemeine Bemerkungen

Das »Datenverarbeitungsregister« (DVR) dient der Transparenz der in Österreich durchgeführten Datenverarbeitungen. Es ist ein öffentliches, jedermann zugängliches, teilweise elektronisch geführtes Register, in das alle meldepflichtigen Datenanwendungen aufgrund einer Meldung des jeweiligen Auftraggebers eingetragen werden. An der Verfügbarkeit des Registers im Internet wird gearbeitet.

Gemäß § 2 Abs. 3 DVRV 2002 besteht die Datenanwendung »Datenverarbeitungsregister« aus:

- den registrierten Meldungen über Auftraggeber und Datenanwendungen
- einem gesonderten Verzeichnis der Informationsverbundsysteme und
- den Registrierungsakten.

Daneben ist das »Datenverarbeitungsregister« auch jene Organisationseinheit (Referat DVR) innerhalb des Geschäftsapparats der DSK, in der die Registrierungsverfahren durchgeführt und auch die das Registrierungsverfahren betreffenden Bescheide der Kommissionsorgane vorbereitet werden.

10.2 Zum Geschäftsgang des Registers

10.2.1 Statistische Aufbereitung

Entsprechend der Gliederung des sonstigen Geschäftsgangs der Datenschutzkommission nach Halbjahren, werden auch Eingänge und Erledigungen im Datenverarbeitungsregister nach Halbjahren gegliedert dargestellt. Die statistischen Auswertungen für den Berichtszeitraum wurden über die Protokollrecherche von DVR-Online erstellt. Die Anzahl der Verbesserungsaufträge bezieht sich oft auf mehrere Datenanwendungen (z.B. mit einer Eingabe werden mehrere Datenanwendungen gemeldet, jene, die mangelhaft sind, werden in einem Verbesserungsauftrag behandelt). Die Anzahl der Enderledigungen ist nachstehend gesondert ausgewiesen.

10.2.2 Wichtige Registrierungen aus dem Berichtszeitraum

10.2.2.1 Informationsverbundsysteme (IVS)

Im Berichtszeitraum registrierte Informationsverbundsysteme im Sinne des § 4 Z 13 DSG 2000 (Auswahl):

- Betreutenverwaltung Caritas Socialis
- Gesundheitsnetz Oberösterreich
- Integrierte Vollzugsverwaltung (IVV)
- LSDB Lohn- und Sozialdumping-Bekämpfung
- Teleradiologienetz Vorarlberg
- Verkehrsunternehmensregister
- WiSion® – Wiener Schulinformationssystem online

10.2.2.2. Sonstige Meldungen

a. Videoüberwachung aus KFZ unzulässig (K600.319-005/0002-DVR/2012, 7.11. 2012)

Sachverhalt:

Der Antragsteller meldete eine Datenanwendung »Videoüberwachung zum Zwecke des Schutzes des überwachten Objekts (Umgebung der Situation im unmittelbaren Bereich des eigenen, privat genutzten PKWs) bzw. der Erfüllung rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung, mit ausschließlicher Auswertung in dem durch die Zweckbezeichnung definierten Anlassfall, sofern bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt könnte das Ziel oder der Ort eines gefährlichen Angriffs werden« zur Registrierung im Datenverarbeitungsregister. Als besondere Rechtsgrundlage wurden die §§ 50a ff DSG 2000 idgF, §§ 353 ff ABGB sowie § 80 StPO angegeben. Als geplante Übermittlungsempfänger nannte der Meldungsleger »Zuständige Behörden bzw. zuständiges Gericht (zur Beweismittellieferung in Strafrechtsangelegenheiten)«, »Sicherheitsbehörden (zu sicherheitspolizeilichen Zwecken)«, »Gerichte (zur Beweismittellieferung in Zivilrechtsangelegenheiten)« und »Versicherungen (zur Abwicklung von Versicherungsfällen)«.

Überdies brachte der Antragsteller vor, die Anwendung diene ausschließlich privaten Zwecken (wie Videokameras auf der Kärntner Straße oder Sportler mit Helmkameras). Eine Videoüberwachung im Sinne einer systematischen, insbesondere fortlaufenden Feststellung von Ereignissen, die ein bestimmtes Objekt oder eine bestimmte Person betreffen, sei nicht gegeben. Im Anlassfall könnten die Aufnahmen aber zur Verfolgung von Straftaten verwendet werden. Die angestrebten Zwecke könnten anders als durch Videoaufnahme nicht erreicht werden. Bezüglich des verlangten statistischen Materials solle man nicht warten, bis etwas passiert, sondern vorausschauend handeln. Es gebe kein konkretes Objekt, das erfasst werden solle. Beim Gehsteig oder der Straße handle es sich nicht um ein Objekt im Sinne des DSG. Es sei kein 24-Stunden-Betrieb vorgesehen. Niemand außer dem Antragsteller habe Zugriff auf die Daten. Private Aufnahmen könnten beliebig lang aufbewahrt werden, die Daten würden zyklisch überschrieben. Die gemeldete Datenanwendung bezwecke nicht die Überwachung des Fahrzeugs in geparktem Zustand, z. B. auf eigenem Grund oder in der eigenen Garage, sondern das Filmen aus dem Fahrzeug heraus und während der Fahrt.

Rechtliche Würdigung:

Die Datenschutzkommission hielt zunächst fest, dass die gegenständliche Datenanwendung den Begriff »Videoüberwachung« in § 50a Abs. 1 DSG 2000 erfüllt. Dies ergibt sich aus Bezeichnung und im Antrag angeführten Rechtsgrundlagen für die Zulässigkeit. Auch die angegebenen Datenarten und Übermittlungsempfänger und somit der gesamte in der Meldung dargestellte Inhalt der Datenanwendung, ebenso wie die skizzierten technischen Anlagen, sprechen dafür. Die Tatsache, dass bei der vorliegenden Videoüberwachungsanlage das »überwachte Objekt« kein stationäres Gebilde (wie etwa ein Haus), sondern ein definierter, aber beweglicher Überwachungsbereich ist (in dem sich immer wieder andere Objekte und Personen befinden), ändert an der grundsätzlichen Anwendbarkeit der §§ 50a ff DSG 2000 nichts. Der Antragsteller übersieht auch, dass der Zweck im Begriff der Videoüberwachung in § 50a Abs. 1 DSG 2000 keine Rolle spielt.

Die – nicht weiter begründete – Behauptung des Antragstellers, dass hier keine systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt oder eine bestimmte Person betreffen, stattfinde, steht mit dem sonstigen Vorbringen in Widerspruch. Danach handelt es sich um eine systematische (Aufzeichnung jeder Fahrt bzw. zumindest bestimmter Arten von Fahrten), insbesondere fortlaufende (Aufzeichnung der gesamten Fahrtstrecke) Feststellung von Ereignissen (Straßenverkehr um sein Fahrzeug), die ein bestimmtes Objekt (sein Fahrzeug) bzw. eine bestimmte Person (jedenfalls den Fahrzeuglenker) betreffen

(es ist nicht Voraussetzung, dass das Objekt bzw. die Person selbst erfasst sind, arg. »betreffen« im Text der Bestimmung). Der Begriff des § 50a Abs. 1 DSG 2000 ist damit erfüllt. Für die Beurteilung der Zulässigkeit der gegenständlichen Anlage ist daher § 50a DSG 2000 (iVm § 6 und § 7 DSG 2000; vgl. § 50a Abs. 2 DSG 2000) einschlägig.

Gemäß § 50a Abs. 2 DSG 2000 sind rechtmäßige Zwecke einer Videoüberwachung, insbesondere der Auswertung und Übermittlung der dabei ermittelten Daten, jedoch vorbehaltlich des Abs. 5 nur der Schutz des überwachten Objekts oder der überwachten Person oder die Erfüllung rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung, im Hinblick auf Ereignisse nach Abs. 1. Wenn der Antragsteller mit Verweis auf Videokameras auf der Kärntner Straße (offenbar zu touristischen Zwecken) bzw. Helmkameras bei Sportlern eine ausschließlich private Datenanwendung und damit § 45 DSG 2000 behauptet, ist ihm entgegen zu halten, dass die von ihm geplante Datenverwendung anderen Zwecken dient, als das Festhalten von Urlaubserinnerungen oder sportlicher Betätigung. Gemäß § 45 Abs. 1 DSG 2000 ist nur die ausschließliche Datenverwendung für persönliche oder familiäre Tätigkeiten unter »private Zwecke« zu subsumieren (umgelegt auf Bildaufnahmen wären dies etwa Hochzeits- oder Urlaubsaufnahmen). Im gegenständlichen Fall ist die Überwachung des Verkehrs bzw. der Umgebung des eigenen Fahrzeugs jedoch von der erkennbaren Intention geprägt, Beweismaterial für die allfällige Übermittlung an Strafverfolgungsbehörden, Gerichte usw zu ermitteln. Dem Antragsteller geht es darum, das ihn bzw. das von ihm gelenkte Fahrzeug betreffende Verkehrsgeschehen aufzuzeichnen, um etwaiges Fehlverhalten (z. B. in die Spur schneiden) festzuhalten oder das Verschulden an Unfallgeschehen aufklären zu können. Seinem Antrag und seiner weiterführenden eigenen Aussage nach ist die Beweissicherung und die Weitergabe der Daten im Anlassfall an Sicherheitsbehörden, Staatsanwaltschaften und Gerichte geplant und damit auch Teilzweck der Datenanwendung. Dies schließt die »ausschließliche« Verwendung für private Zwecke, wie § 45 DSG 2000 verlangt, nach geltender Rechtslage jedenfalls aus. Ferner wird darauf hingewiesen, dass Datenanwendungen, die unter § 45 DSG 2000 fallen, gemäß § 17 Abs. 2 Z 4 gar nicht der Meldepflicht unterlägen. Zweck der geplanten Videoüberwachung ist der Schutz des eigenen Fahrzeugs bzw. der eigenen Person als Lenker des Fahrzeugs (einschließlich der Beweissicherung). Der Zweck ist daher von § 50a Abs. 2 DSG 2000 erfasst.

Nach dieser Bestimmung gelten für Videoüberwachung aber auch (wie bei jeder Datenanwendung) die §§ 6 und 7 DSG 2000. Gemäß § 7 Abs. 1 DSG 2000 dürfen Daten nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und ferner die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzt werden.

Hinsichtlich der generellen Befugnis zur Durchführung einer Videoüberwachungsanlage orientiert sich die grundsätzliche Berechtigung eines privaten Auftraggebers an dessen Verfügungsbefugnis über den im Einzelfall konkret zu überwachenden Raum. Private dürfen daher regelmäßig nur jene Bereiche überwachen, an denen ihnen ein hausrechtsähnliches Verfügungsrecht zukommt; also etwa das eigene Haus, den eigenen Garten oder das eigene Betriebsgelände. Eine solche Verfügungsbefugnis kann sich dabei sowohl aus einem Eigentumsrecht, aber auch etwa aus einem Mietverhältnis ergeben. In Abgrenzung dazu sind an »öffentlichen Orten« (im Sinne des § 27 SPG) aufgrund des staatlichen Gewaltmonopols grundsätzlich nur die Sicherheitsbehörden zur Durchführung von Videoüberwachungen berechtigt und richtet sich deren Zulässigkeit nach den Anforderungen des SPG (vgl. § 54 Abs. 6 und 7 SPG). Da die im Fahrzeug des Antragstellers montierte Kamera während der Fahrt regelmäßig sowie in beabsichtigter und umfassender Weise öffentlichen Raum erfassen würde, fehlt es dem Antragsteller bereits an der hierfür erforderlichen »gesetzlichen Zuständigkeit« bzw. »rechtlichen Befugnis« im Sinne des § 7 Abs. 1 DSG 2000.

Auf die Frage, ob gegenständlich schutzwürdige Geheimhaltungsinteressen der Betroffenen (also der erfassten Verkehrsteilnehmer) verletzt würden, was für Videoüberwachung in § 50a Abs. 3 und 4 DSG 2000 geregelt ist, musste daher nicht mehr eingegangen werden.

Ferner wird darauf hingewiesen, dass bei der Beurteilung der Verhältnismäßigkeit des Grundrechtseingriffes durch eine geplante Videoüberwachung auch stets die betroffenen Örtlichkeiten und die einzelnen Kamerastandorte mit zu berücksichtigen sind. Dies ist bei mobilen Kameras ex ante naturgemäß schwer möglich bzw. wäre hier quasi eine »Blankogenehmigung« jedes denkmöglichen Standortes im Voraus notwendig. Aus diesem Grund ist der geplante Einsatz einer mobilen Videoüberwachungsanlage in einem Kfz (auch) als unverhältnismäßig im Sinne des § 7 Abs. 3 DSG 2000 anzusehen.

Die Registrierung wurde daher abgelehnt.

b. Whistleblowing und Betriebsvereinbarungen (K600.320-005/0003-DVR/2012, 14.12. 2012)

Sachverhalt:
Die A GmbH hat die Datenanwendung mit der Bezeichnung »Hinweisgebersystem«, die zur Einrichtung eines internen Verfahrens zur Meldung von Missständen dient, beim Datenverarbeitungsregister gemeldet.

Meldungen von Missständen können dabei auf zwei unterschiedliche Arten eingebracht werden: Einerseits kann ein Mitarbeiter der Auftraggeberin eine Meldung an den lokalen Compliance Officer der Auftraggeberin erstatten. Der Compliance Officer hat die Einordnung der jeweiligen Meldung dahingehend vorzunehmen, ob es sich um einen schweren Verstoß im Sinne der schriftlich vorgelegten Unternehmensrichtlinie handelt, der auf Konzernebene bearbeitet werden muss, oder um eine leichte Verfehlung, die lokal untersucht wird. Soweit sich die Meldung auf einen schweren Verstoß bezieht, werden die Meldungen von der Auftraggeberin an die Konzernmutter in Deutschland zur Verfolgung übermittelt.

Andererseits sollen Mitarbeiter die Möglichkeit haben, eine direkte Meldung mutmaßlicher Missstände an die Konzernmutter in Deutschland zu erstatten.

Meldungen in den (im Bescheid abschließend, hier aber nur beispielhaft wiedergegebenen) folgenden Bereichen gelten laut Unternehmensrichtlinie als schwere Verstöße: Verstoß (oder Teilnahme daran) gegen Vorschriften der ordnungsgemäßen Rechnungslegung und Buchhaltung, Verstoß gegen interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Korruption, Bestechung, Betrug (soweit der mutmaßliche Vermögensschaden einen Wert von € 50.000 übersteigt), Geldwäsche, Insiderhandel, sonstige Finanzkriminalität (soweit der mutmaßliche Vermögensschaden einen Wert von € 50.000 übersteigt) etc.

Alle übrigen Verstöße, die in der Unternehmensrichtlinie zum Hinweisgebersystem angeführt sind, werden an die Antragstellerin als Arbeitgeberin zur normalen Bearbeitung zurückgeleitet, egal wie sie gemeldet wurden.

Auf Anfrage der Datenschutzkommission nach einer Betriebsvereinbarung hat die Antragstellerin ein Schreiben ihres Betriebsausschusses vorgelegt, in dem dieser die Meinung vertritt, dass das gegenständliche Hinweisgebersystem ohne Betriebsvereinbarung eingeführt werden könne. Der Betriebsausschuss verzichtete ausdrücklich auf den Abschluss einer diesbezüglichen Betriebsvereinbarung.

Rechtliche Würdigung:
Die Meldung der Datenanwendung umfasst strafrechtlich relevante Daten gem § 18 Abs. 2 Z 2 DSG 2000 und unterliegt damit der Vorabkontrolle. Dabei kann die Datenschutzkommission dem Auftraggeber Auflagen für die Vornahme der Datenanwendung durch Bescheid erteilen.

Hinsichtlich der Übermittlung von Daten im Internationalen Datenverkehr an die Konzernmutter in Deutschland besteht Genehmigungsfreiheit, da dieses Unternehmen seinen Sitz in einem EWR-Land hat (§ 12 Abs. 1 DSG 2000). Eine Genehmigung gem § 13 DSG 2000 war daher nicht erforderlich.

Da die Mitarbeiter bei (elektronisch aufgezeichneten) Meldungen in das Hinweisgebersystem letztlich in Erfüllung der für sie verpflichtenden unternehmensinternen Verhaltensregeln tätig werden, sind ihnen derartige Meldungen nicht als Privatperson, sondern als Organ des Unternehmens zuzurechnen, sodass datenschutzrechtlich handelndes Rechtssubjekt das Unternehmen ist. Der Antragstellerin ist daher die Eigenschaft eines Auftraggebers für die Verwendung von gemeldeten Missbrauchsdaten zuzuerkennen, die (elektronischen) Aufzeichnungen stellen eine Datenanwendung der Antragstellerin dar.

Zur Rechtsgrundlage der beantragten Übermittlungen:

Wie im Sachverhalt ausgeführt, sind Maßstab für den zu meldenden »Missbrauch« die konzerninternen Verhaltensregeln. Für die Mitarbeiter der Antragstellerin haben diese Regeln durch die Unternehmensrichtlinie zum Hinweisgebersystem, in der das Recht und auch die Aufforderung zur Meldung von schwerwiegenden Verstößen festgehalten sind, rechtliche Relevanz. Verstöße gegen diese Verhaltensregeln werden daher zumindest arbeitsrechtlich nicht irrelevant sein, sodass dem Arbeitgeber ein überwiegendes berechtigtes Interesse an der Kenntnis von solchen Verstößen zuzubilligen ist.

Die Datenschutzkommission geht regelmäßig davon aus, dass es sich bei Kontrollsystemen wie dem hier einzuführenden um solche handelt, die den Mitwirkungsrechten der §§ 96, 96a ArbVG unterliegen. Diese Bestimmungen sind nicht disponibel und daher unabhängig von der Einschätzung des Betriebsrats einzuhalten, um dadurch auch die »Rechtmäßigkeit« der Datenanwendung als Voraussetzung für die datenschutzrechtliche Genehmigung herzustellen. Die von der Auftraggeberin dazu vertretene Auffassung, die von ihr geplante Maßnahme unterliege nicht den Mitwirkungsrechten des Betriebsrats, weil die Auftraggeberin ihre Mitarbeiter nicht zur Überwachung auffordere, sondern ihnen nur eine Möglichkeit der Meldung illegalen Verhaltens anbiete, überzeugt nicht. Dazu genügt schon der Hinweis auf den von der Auftraggeberin vorgelegten Verhaltenskodex, aus dem hervorgeht, dass »Mitarbeiter [...] darin bestärkt und dazu angehalten [werden], mögliche Verletzungen des Verhaltenskodex mitzuteilen«.

Ein überwiegendes berechtigtes Interesse der Konzernspitze an der Kenntnis von allen Verstößen gegen die konzerninternen Verhaltensregeln wird demgegenüber nicht anzunehmen sein, da dies unverhältnismäßig wäre. Eine sachliche Rechtfertigung für die Übermittlung von Missbrauchsdaten zum Zweck der Aufklärung und Untersuchung von Vorfällen wird nur dann anzunehmen sein, wenn dieser Zweck bei der Antragstellerin selbst nicht zweifelsfrei erreicht werden kann: Im Umfang der Meldung von maßgeblichen Verstößen, die Mitarbeitern der Antragstellerin in Führungspositionen oder vergleichbar hochgestellten Positionen angelastet werden, anerkennt die Datenschutzkommission das Bestehen eines überwiegenden berechtigten Interesses an der Übermittlung der Meldungsdaten an die Konzernspitze, da nur auf diese Weise mit hinlänglicher Sicherheit eine objektive und vollständige Aufklärung der erhobenen Vorwürfe zu erwarten ist. Die Meldung von Vorfällen, die keine leitenden Angestellten betreffen, wäre nicht zulässig, weil

in solchen Fällen die Antragstellerin selbst ohne Hilfe der Konzernmutter das Problem bereinigen kann. In dem Fall, dass ein Mitarbeiter von geringerem Einfluss auf die Unternehmensführung einen schwerwiegenden Verstoß verursacht, wäre eine Meldung an die Konzernspitze dann zulässig, wenn die Vorgesetzten ihre Aufsichtspflicht nicht korrekt wahrnehmen und dadurch ihrerseits maßgeblich gegen die Konzernrichtlinien verstoßen.

Die Zulässigkeit der Übermittlung von Missbrauchsdaten bedarf angesichts ihres hohen Schadenspotentials für den Beschuldigten besonderer Begleitmaßnahmen, um eine Verletzung von Datenschutzrechten hintanzuhalten. Die Antragstellerin hat jene organisatorischen Begleitmaßnahmen im Antrag beschrieben, die im antragsgegenständlichen internen Verfahren zum Schutz von Betroffenenrechten vorgesehen sind. Sie entsprechen weitgehend jenen besonderen Garantien, die in der Äußerung WP 117 der Art. 29 Gruppe für eine datenschutzkompatible Führung einer »whistleblowing hotline« verlangt werden.

Die Registrierung der Datenanwendung wurde daher unter folgenden Auflagen verfügt:

1. Die Übermittlung von personenbezogenen Daten von Beschuldigten ist nur hinsichtlich leitender Angestellter zulässig, die eines maßgeblichen Verstoßes (oder der Teilnahme daran) gegen die konzernintern verbindlichen Regelungen betreffend die im Sachverhalt angeführten schweren Verstöße bezichtigt werden.
2. Die mit der Bearbeitung von Meldungen betraute Stelle ist von den anderen Konzernstellen strikt getrennt und hat nur Personen als Mitarbeiter, die besonders geschult und für die Vertraulichkeit der gemeldeten Daten ausdrücklich verantwortlich sind.
3. Die Antragstellerin lässt anonyme Meldungen zwar zu, fördert sie aber nicht, sondern sichert vielmehr den Meldern volle Vertraulichkeit hinsichtlich ihrer Identität zu, wenn sie diese angeben.
4. Die Beschuldigten haben grundsätzlich Zugang zu Anschuldigungen.
5. Die Identität des Meldenden wird nur dann offengelegt, wenn sich nachträglich herausstellt, dass die Anschuldigung bewusst falsch erhoben wurde.
6. Die eingemeldeten Daten werden spätestens 2 Monate nach Beendigung der Untersuchung gelöscht.
7. Die Registrierung ist an die Auflage geknüpft, dass die Mitarbeiter im Arbeitsvertrag oder sonst durch generelle Weisung zur Einhaltung der der Behörde vorgelegten Unternehmensrichtlinie zum Hinweisgebersystem und zur Meldung an den Arbeitgeber über wahrgenommene Verstöße gegen diesen Code verpflichtet wurden.
8. Die Registrierung wird unter der aufschiebenden Bedingung verfügt, dass eine dem Sachverhalt angemessene Betriebsvereinbarung abgeschlossen wird.

10.3 DVR-Online

Seit 1. September 2012 dürfen Meldungen an das Datenverarbeitungsregister grundsätzlich nur mehr über die Internet-Applikation »DVR-ONLINE« vorgenommen werden. Die Rechtsgrundlage hierfür bildet § 17 Abs. 1a DSG 2000.

§ 17 Abs. 1a DSG 2000 lautet:

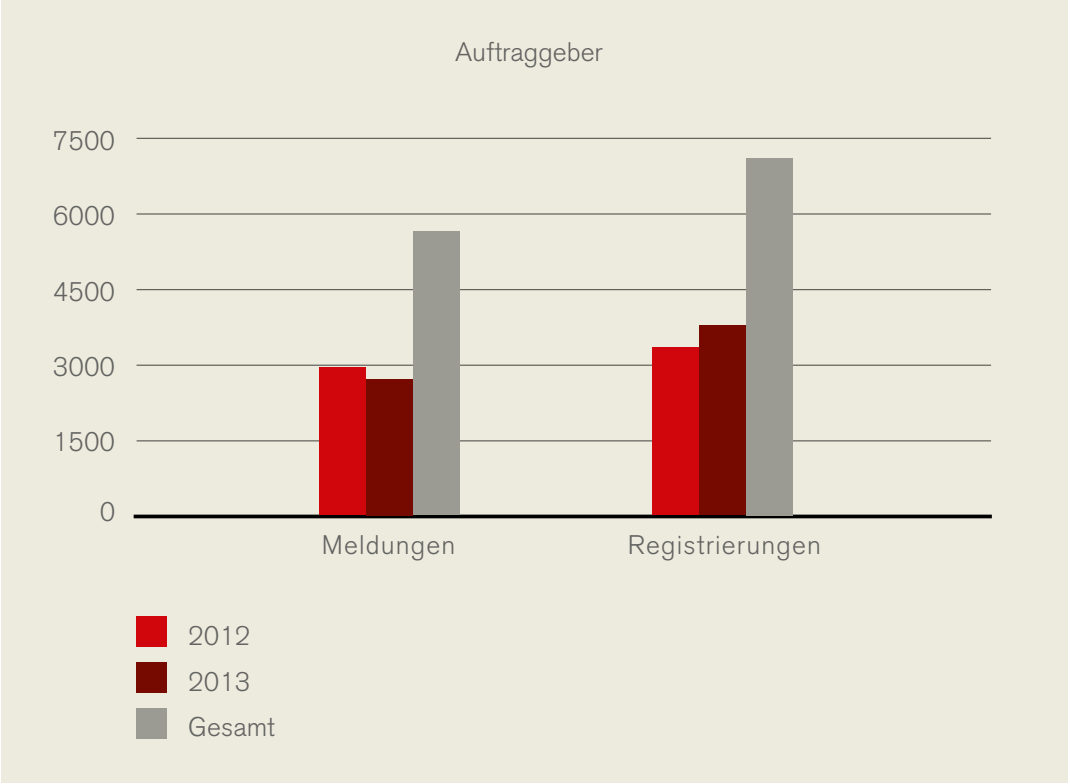
»Die Meldung ist in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen. Die Identifizierung und Authentifizierung kann insbesondere durch die Bürgerkarte (§ 2 Z 10 des E-Government-Gesetzes, BGBl. I Nr. 10/2004) erfolgen. Nähere Bestimmungen über die Identifizierung und Authentifizierung sind in die gemäß § 16 Abs. 3 zu erlassende Verordnung aufzunehmen. Eine Meldung in Form von E-Mail oder in nicht-elektronischer Form ist für manuelle Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig.«

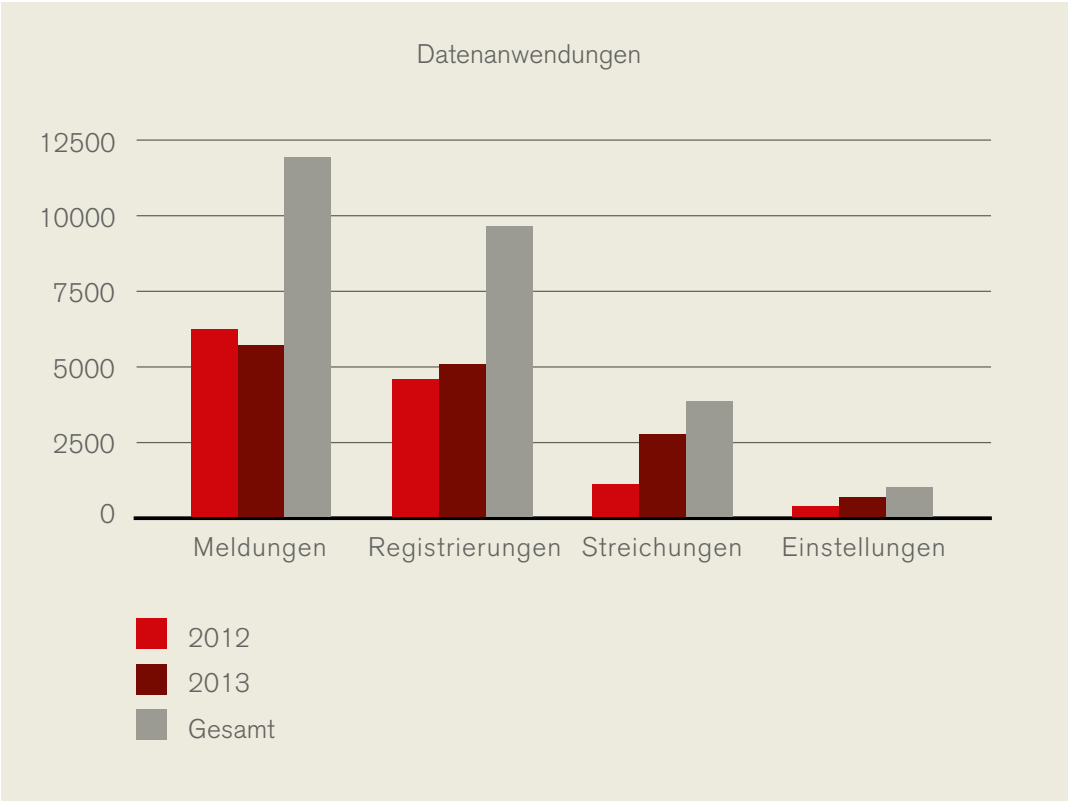
Für eine Meldung beim Datenverarbeitungsregister gibt es verschiedene sichere Zugangsmöglichkeiten. Damit ist sichergestellt, dass nur berechtigte Personen einen direkten Zugang zum Meldebereich des Auftraggebers erlangen und DVR-Meldungen erstatten können.

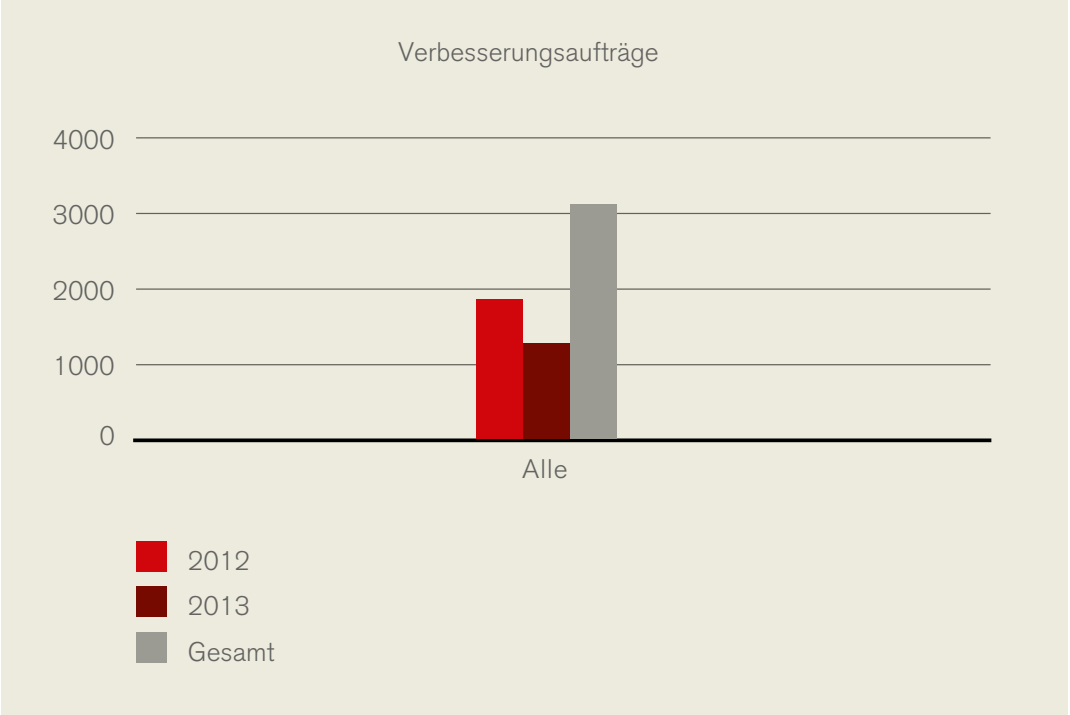
Zugangsmöglichkeiten zur DVR-Online-Applikation:

a. Unternehmen, Vereine: Unternehmen, Einzelunternehmer, Vereine können über das Unternehmensserviceportal (www.usp.gv.at) oder über das DVR-Portal in DVR-Online einsteigen.
b. Einzelpersonen: Einzelpersonen, die nicht unternehmerisch tätig sind, können über das DVR-Portal in DVR-Online einsteigen.
c. Behörden: Behörden erreichen DVR-Online über den Behörden-Portalverbund.
d. Berufsmäßige Parteienvertreter: Rechtsanwälte und Notare erreichen DVR-Online mit ihrem elektronischen Berufsausweis.

Nach ursprünglichen Anlaufschwierigkeiten, vor allem bedingt durch gewisse Verständnisprobleme hinsichtlich der Erlangung einer Zugangsberechtigung im Vorfeld der DVR-Online-Applikation, hat sich die Zahl der Meldungen bereits wieder nach kurzer Zeit auf das »übliche« Ausmaß eingependelt. Vom 1. September 2012 bis zum 31. Dezember 2013 wurden 2.777 neue DVR-Nummern an erstmalig meldende Auftraggeber vergeben. Die Anzahl der seit Einführung von DVR-Online eingelangten Datenanwendungen beträgt 7.926. Von diesen Datenanwendungen wurden lediglich 1.747 vom System automatisch registriert (keine Vorabkontrollfälle), somit etwas mehr als ein Fünftel anstatt der ursprünglich angestrebten fünfzig Prozent. Die erwünschte spürbare Entlastung des Datenverarbeitungsregisters ist somit auch durch die Einführung von DVR-Online nicht eingetreten. Gründe hierfür: Sehr oft wurde von den Auftraggebern im Online-Meldeformular angegeben, dass es sich bei der Datenanwendung um einen Fall der Vorabkontrolle handelte, was jedoch nicht den Tatsachen entsprochen hat. In vielen weiteren Fällen konnte auch aus systemtechnisch bedingten Gründen die vorgesehene automatische Registrierung durch das DVR-Online-System nicht erfolgen (etwa wenn gleichzeitig eine Auftraggeber-Änderungsmeldung erfolgte oder bereits eine noch nicht registrierte Auftraggeber-Meldung existierte).


Auftraggeber
7500
6000
4500
3000
1500
0
Meldungen
Registrierungen
2012
2013
Gesamt


Datenanwendungen
12500
10000
7500
5000
2500
0
Meldungen
Registrierungen
Streichungen
Einstellungen
2012
2013
Gesamt


Verbesserungsaufträge
4000
3000
2000
1000
0
Alle
2012
2013
Gesamt

11 Die Datenschutzkommission als Stammzahlenregisterbehörde

11.1 Die Funktionen der Stammzahlenregisterbehörde

11.1.1 Bereichsspezifische Personenkennzeichen

Im österreichischen E-Government-System erfolgt die eindeutige Identifikation von natürlichen Personen durch eine geheime Stammzahl und davon abgeleitete bereichsspezifische Personenkennzeichen (bPK). Die Stammzahl darf nur auf der Bürgerkarte gespeichert werden. Sie wird aus der im zentralen Melderegister verwendeten ZMR-Zahl mit Hilfe eines geheimen Schlüssels gebildet. Der geheime Schlüssel und alle damit verknüpften Funktionen werden von der DSK in ihrer Funktion als Stammzahlenregisterbehörde verwaltet. Die für das Funktionieren des bereichsspezifischen eindeutigen Identifikationssystems im österreichischen E-Government erforderlichen Datenanwendungen: das Stammzahlenregister, das Ergänzungsregister für natürliche Personen, das Ergänzungsregister für sonstige Betroffene und das Vollmachtenregister werden von der Datenschutzkommission als Auftraggeber im datenschutzrechtlichen Sinn betrieben.

Die Stammzahlenregisterbehörde erzeugt bereichsspezifische Personenkennzeichen, stellt Anwendungen zur Erzeugung von bereichsspezifischen Kennzeichen auf Grundlage der Stammzahl zur Verfügung und stellt sicher, dass diese richtig eingesetzt werden. Zu diesem Zweck müssen Auftraggeber des öffentlichen Bereichs einen Antrag bei der Stammzahlenregisterbehörde auf Erlaubnis der Ausstattung einer Datenanwendung mit bPKs stellen. Anlässlich der Erlaubniserteilung wird von der Stammzahlenregisterbehörde festgelegt, welchem Bereich die Datenanwendung zuzurechnen ist und mit welcher Bereichskennung daher die bPKs für diese Datenanwendung zu bilden sind.

Dieses im österreichischen E-Government eingesetzte System der bereichsspezifischen Personenkennzeichen stellt sicher, dass die eindeutig erzeugten Identifikatoren für ein- und dieselbe Person in unterschiedlichen Bereichen der öffentlichen Verwaltung unterschiedlich sind, innerhalb dieses Bereiches aber eindeutig. Das erleichtert der öffentlichen Verwaltung die Zuordnung von Personen zu Verfahren, erlaubt es den betroffenen Bürgern mit einem einzigen sicheren Mechanismus immer mehr öffentliche Dienstleistungen bequem elektronisch abzuwickeln und schützt gleichzeitig die betroffenen Bürger vor einer leichteren Zusammenführbarkeit ihrer Daten durch die Einführung von Personenkennzeichen. Ein bereichsspezifisches Personenkennzeichen kann weder auf die Stammzahl zurückgerechnet werden, noch – ohne zusätzliche Angaben über die Person und der Mitwirkung der Stammzahlenregisterbehörde – in ein bereichsspezifisches Personenkennzeichen eines anderen Bereichs umgerechnet werden.

11.1.2 Ergänzungsregister

Die DSK betreibt in ihrer Funktion als Stammzahlenregisterbehörde zwei Register, in die sich jene natürlichen Personen und sonstige rechtlich erhebliche Entitäten (z. B. Behörden oder ARGEs) eintragen lassen können, die in keinem der Basisregister des E-Governmentsystems (Firmenbuch, Zentrales Melderegister oder Vereinsregister) eingetragen sind.

In das Ergänzungsregister für natürliche Personen können Personen eingetragen werden, die nicht im zentralen Melderegister eingetragen werden müssen. Dadurch kann bei Bedarf für jede Person ein bereichsspezifisches Kennzeichen errechnet werden.

In das Ergänzungsregister für sonstige Betroffene kann jedes Unternehmen eingetragen werden, das nicht im Firmenbuch oder Vereinsregister erfasst werden muss. Unternehmen und juristische Personen werden im österreichischen E-Government nicht durch bereichsspezifische Kennzeichen eindeutig identifiziert, sondern mit bereichsübergreifenden Kennzeichen, die zum

Teil auch offen geführt werden, wie z. B. die Firmenbuchnummer. Diese Kennzeichen werden in E-Government Anwendungen als Stammzahl verwendet. Das Ergänzungsregister für sonstige Betroffene schließt die Lücke für jene Unternehmen, die in Österreich kein Kennzeichen haben. Dadurch kann für jedes Unternehmen eine Stammzahl gebildet werden.

11.1.3 Vollmachtenregister

Schließlich betreibt die DSK in ihrer Funktion als Stammzahlenregisterbehörde das Vollmachtenregister. Es erlaubt vertretungsweises Handeln in E-Government Anwendungen. Es wurde aus budgetären Gründen nur rudimentär entwickelt und belastet die Behörde mit manuellen Überprüfungen und Eintragungen. In Konkurrenz zu diesem System wurde vom Finanzministerium das Unternehmensserviceportal (USP) in Betrieb genommen, das Unternehmen eine ähnliche Funktionalität in für große Unternehmen leichter zugänglicher Form anbietet.

11.2 Entwicklungen

11.2.1 Bereichsspezifische Kennzeichen für die Verwendung im privaten Bereich

Die wichtigste Neuerung der Novelle zum E-Government-Gesetz (BGBl. I Nr. 7/2008) bestand darin, dass Banken und Versicherungen unter gewissen Voraussetzungen bereichsspezifische Personenkennzeichen verwenden dürfen. Dadurch könnte einerseits die Qualität der Identitätsdaten der Kunden dieser Unternehmen erheblich verbessert werden, zum anderen wäre der Zugang zum Electronic Banking technisch wesentlich besser absicherbar als mit den derzeit üblichen PINs und TANs oder der TAC Systeme. Mit einem gemeinsamen Zugangssystem für Angebote der öffentlichen Verwaltung und der Privatwirtschaft würde auch das Problem des Merkens von unterschiedlichen Passwörtern für die unterschiedlichen Zugangssysteme erheblich entschärft werden. Von diesem Angebot haben diese Unternehmen allerdings bisher keinen Gebrauch gemacht.

11.2.2 Organisatorische und personelle Probleme

Im letzten Datenschutzbericht hat die Datenschutzkommission bemängelt, dass die Stammzahlenregisterbehördenverordnung 2009, BGBl. II Nr. 330/2009 und die Ergänzungsregisterverordnung 2009 BGBl. II Nr. 331/2009 die Kompetenzen und den Handlungsspielraum der Stammzahlenregisterbehörde zwar erweitert haben, aber scheinbar davon ausgegangen wurde, dass die mit diesen Kompetenzen verknüpften E-Government-Funktionen selten genützt werden. Daher müssen viele Anträge manuell behandelt werden, wofür ihre Personalausstattung nicht ausreicht.

Gleiches gilt auch für die aus datenschutzrechtlicher Sicht wichtigen Kontrollen von öffentlichen und privaten Einrichtungen, die bereichsspezifische Personenkennzeichen verwenden. In diesem Bereich wurde im letzten Datenschutzbericht eingefordert, dass diese Kontrollen sowohl durch technische Maßnahmen, personelle Verstärkung als auch durch Heranziehung weiterer Dienstleister für technische Kontrollen gewährleistet werden muss.

Im Berichtszeitraum hat sich das Angebot von E-Government Anwendungen stark vergrößert und auch die Nutzung dieses Angebots nimmt stetig zu. Der DSK steht aber für die Bewältigung der damit verbundenen Aufgaben am Ende des Jahres 2013 weiterhin nur ein halber Mitarbeiter zur Verfügung. Mit diesen Ressourcen konnte die Behörde ursprünglich den Pilotbetrieb nur mit großer Anstrengung aufrechterhalten. Im Berichtszeitraum ist eine regelmäßige Führung / Überwachung der Dienstleister der Behörde, die täglich hunderttausende Personenkennzeichen für die DSK ausstellen, kaum noch leistbar. Im Bereich des operativen Betriebs

der Behörde kommt es durch die angespannte Personalsituation zu erheblichen Rückständen und Verzögerungen bei der Bearbeitung von Anträgen und Anfragen.

Das E-Government Großprojekte der Einführung der Transparenzdatenbank hatte daher schwerwiegende Folgen für die Stammzahlenregisterbehörde. Allein die durch dieses Projekt ausgelösten Anfragen und notwendigen Koordinationsmaßnahmen lasteten die Behörde zur Gänze aus. Das sorgte für eine sprunghafte Zunahme von Bearbeitungsrückständen und beinahe zum faktischen Kontrollverlust über die Dienstleister der Behörde. Die Datenschutzkommission erinnert in diesem Zusammenhang daran, dass Auftraggeber von Datenanwendungen diese nur solange betreiben dürfen, wie sie sicherstellen können, dass die im DSG 2000 verankerten Grundsätze eingehalten werden und dass alle Bestimmungen über die einzuhaltenden Datensicherheitsmaßnahmen sowohl vom Auftraggeber als auch von den Dienstleistern befolgt werden.

Sofern der Wunsch besteht, dass die Datenschutzbehörde diese Datenanwendungen weiterhin betreibt, müssen ihr die dafür notwendigen Ressourcen zur Verfügung gestellt werden. Gleiches gilt für die Bearbeitung von Anträgen, für die nahezu keine Personalressourcen zur Verfügung stehen.

11.2.3 Zahlen

In den Jahren 2011, 2012 und 2013 wurden von der Stammzahlenregisterbehörde

- 338.716.219 (Stand 3.12.2013) bereichsspezifische Personenkennzeichen berechnet,
- 1056 (Stand 3.12.2013) Vollmachten in das Vollmachtenregister eingetragen,
- über 12.000 (Stand 30.5.2013) neue Personen in das Ergänzungsregister für natürliche Personen eingetragen und
- etwa 1,4 Millionen Eintragungen in das Ergänzungsregister für sonstige Betroffene vorgenommen.

11.3 Behördenstruktur, Neuerungen und Veränderungen

11.3.1 Verbesserung der technischen Einrichtungen und der Zusammenarbeit mit und zwischen den Dienstleistern der Stammzahlenregisterbehörde

Neben der DSK als verantwortlicher Behörde sind für die DSK mehrere Bundesministerien als Dienstleister und auch private Unternehmen als Subdienstleister tätig. Sowohl der Betrieb der Datenanwendungen als auch die Steuerung der Arbeitsabläufe der Stammzahlenregisterbehörde, die sich auf viele Personen, die bei unterschiedlichen Behörden und Unternehmen beschäftigt sind, stellt daher eine ständige besondere Herausforderung dar.

Im Berichtszeitraum war die Stammzahlenregisterbehörde daher neben der Führung und Überwachung des laufenden Betriebs der verschiedenen technischen Einrichtungen und der mit der Umsetzung beauftragten Dienstleister sowie der Betreuung öffentlicher Auftraggeber im Zusammenhang mit der Ausstattung ihrer Datenanwendungen mit bereichsspezifischen Personenkennzeichen, vor allem bestrebt, die Struktur der Arbeitsabläufe zu verbessern und technische Hilfsmittel zu entwickeln, die zur besseren Steuerung und Bewältigung der Aufgaben im Umfeld der besonderen personellen Struktur der Stammzahlenregisterbehörde beitragen.

Leider war das im Berichtszeitraum kaum möglich, da alle Ressourcen zur Bewältigung von dringenden Aufgaben eingesetzt werden mussten. Daher können in diesem Bericht nur einige wenige Neuerungen vorgestellt werden.

11.3.2 Neuerungen

Stammzahlenregister

Neben Funktionen zur besseren Darstellung der Verwendung von bPK wurde vom Bundesministerium für Inneres im Auftrag der DSK damit begonnen eine Datenanwendung zur automatischen Kontrolle des Abfragens von bPKs über die Behördenschnittstelle zu entwickeln. In Zukunft soll mit dieser Datenanwendung das unberechtigte Abfragen von bPK durch Behörden erheblich erschwert werden.

Volmachtenregister

Die hinter dem Vollmachtenregister stehende Datenanwendung wurde mit rudimentären Kontrollfunktionen für die DSK ausgestattet und soweit wie möglich an die Bedürfnisse der Benutzer angepasst.

Ergänzungsregister für sonstige Betroffene

Das Ergänzungsregister für sonstige Betroffene verwendet nun die GLN (global location number) als Ordnungsnummer. Anträge auf Eintragung oder Änderung eines Eintrags können nun auch durch Betroffene selbst mittels eines bürgerkartentauglichen Formulars gestellt werden.

11.3.3 Organisatorische Änderung beim Ergänzungsregister für sonstige Betroffene (ERsB)

Die Datenschutzkommission bedient sich fortan der Bundesanstalt Statistik Österreich als Dienstleister für das ERsB. Durch eine Fusion mit dem Teil des Unternehmensregisters, der nicht auf Basis des Firmenbuchs oder Vereinsregisters erstellt wurde, ist das ERsB mit 1,4 mio eingetragenen sonstigen Betroffenen zum größten österreichischen Unternehmensregister angewachsen.